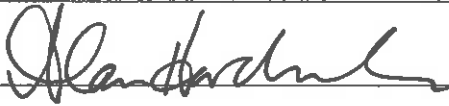


**POLICE AND CRIME COMMISSIONER (PCC) FOR LINCOLNSHIRE  
REQUEST FOR DECISION**

REF: 016/2015  
DATE: 13 May 2015

SUBJECT	INFORMATION AGREEMENT	ASSURANCE	REGIONAL
REPORT BY	Chief Constable Neil Rhodes		
CONTACT OFFICER	Richard Burge, IMU Manager Telephone 01522 947100		
<b>EXECUTIVE SUMMARY AND PURPOSE OF REPORT</b> <p>This Regional Information Assurance document has been written for the purpose of all Regional Collaboration initiatives. It details the terms and conditions under which Police Data may be shared, processed and the general responsibilities of each Data Controller and Data Processor. It is a generic document that covers all collaboration projects but with bespoke schedules that for example detail Information Management, who is party to the collaboration, and the purpose of the collaboration.</p> <p>The document has been reviewed and agreed by the Regional Information Assurance Group (RIAG). All Regional Information Assurance leads attend RIAG and have used their knowledge and experience to assist in formulating this Agreement and ensuring all Information Assurance requirements are met and adhered to.</p> <p>Having this Agreement in place will reduce the risk of any security breaches and gives clear guidelines on how the information shared can be utilised and protected. This will give reassurance to the public on how forces operate and protect their information. It will also give reassurance to the Information Commissioner's Office (ICO) that if a breach does occur, as a Regional we have considered and set down guidelines on how we should manage information in collaboration.</p>			
RECOMMENDATION	<i>That this document is approved and implemented for all Regional Collaborations</i>		

<b>POLICE AND CRIME COMMISSIONER FOR LINCOLNSHIRE</b>	
I hereby approve the recommendation above, having considered the content of this report.	
Signature: 	Date: 13/05/15

**A. NON-CONFIDENTIAL FACTS AND ADVICE TO THE PCC**

This Regional Information Assurance Document outlines the requirements the Information assurance requirements for each force when entering into regional collaboration. It also sets out the terms and conditions under which Police Data may

be shared between the Parties, which Personal Data will be processed by the Data Processor and the general responsibilities of each Data Controller and Data Processor. The document has been heavily influenced by Lincolnshire Police Information Assurance professionals and provides the necessary guidance to ensure each force complies to national standards when processing and sharing information, as such it is recommended it be adopted for all forces and be signed by the PCC.

## **A1. INTRODUCTION AND BACKGROUND**

1. This document was formulated and produced to provide a consistent approach to Information Assurance across the region thereby providing assistance to the numerous collaboration initiatives that are now taking place. It was formulated and agreed at the Regional Information Assurance Group (RIAG), chaired by the DCC of Nottinghamshire, and in which Lincolnshire plays an active part. It is believed that the implementation of this document will enable such collaboration initiatives to be implemented more effectively and within tight timeframes often required. It has been devised as a generic agreement that covers all collaboration initiatives, negating the need for individual agreements going forward.
2. As stated the Information Assurance leads within Lincolnshire have been heavily involved in the writing of this Agreement. Additionally we have held meetings with the author of the Agreement to ensure it fits all Regional Forces needs and compliance requirements for Information Security, Data Protection and Information Assurance.
3. The document will have a bespoke Schedule 5 and Schedule 6 for each Collaboration initiative. Schedule 5 will detail Information Management information in relation to Freedom of Information, Confidentiality, Data Protection, Data Security and Risk Management. Schedule 6 will detail who is party to the Collaboration, its purpose along with details of the data controller for the information involved.

## **A2. LINKS TO POLICE AND CRIME PLAN AND PCC'S STRATEGIES/PRIORITIES**

By ensuring that the information all regional forces hold and process in any regional project meets all the required standards it will link to following strategies/priorities.

- Reduce Crime
- A fair deal for the people of Lincolnshire

## **B. FINANCIAL CONSIDERATIONS**

None

## **C. LEGAL AND HUMAN RIGHTS CONSIDERATIONS**

*[This should include the legal powers the PCC has for making the decision]*

None

## **D. PERSONNEL AND EQUALITIES ISSUES**

None

**E. REVIEW ARRANGEMENTS**

The document will be subject to review at the Regional Information Assurance Group when necessary and required.

**F. RISK MANAGEMENT**

None

**H. PUBLIC ACCESS TO INFORMATION**

Information in this form along with any supporting material is subject to the Freedom of Information Act 2000 and other legislation. Part 1 of this form will be made available on the PCC's website within one working day of approval. However, if release by that date would compromise the implementation of the decision being approved, publication may be deferred. An explanation for any deferment must be provided below, together with a date for publication.

**Is the publication of this form to be deferred? No**

**If Yes, for what reason:**

**Until what date:**

Any facts/advice/recommendations that should not be made automatically available on request should not be included in Part 1 but instead on the separate part 2 form.

**Is there a part 2 form? No**

**If Yes, for what reason:**

**ORIGINATING OFFICER DECLARATION**

Originating Officer:

Richard Burge recommends this proposal for the reasons outlined

Initial to confirm

 RB

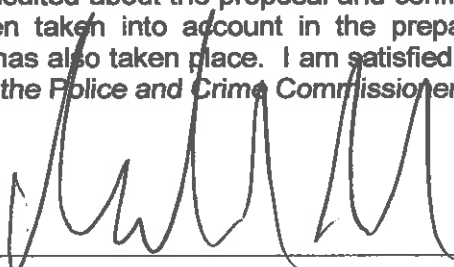
above.	
Financial advice: The PCC's Chief Finance Officer has been consulted on this proposal.	ay
The CC's Chief Finance Officer has been consulted on this proposal.	<del>AY</del>
Monitoring Officer: The PCC's Monitoring Officer has been consulted on this proposal	<del>MO</del>
Chief Constable: The Chief Constable has been consulted on this proposal	<del>MC</del>

## OFFICER APPROVAL

### **Chief Executive**

I have been consulted about the proposal and confirm that financial, legal and equalities advice has been taken into account in the preparation of this report. Consultation outlined above has also taken place. I am satisfied that this is an appropriate request to be submitted to the Police and Crime Commissioner for Lincolnshire.

**Signature:**



**Date:**

13/5/15

## **REGIONAL INFORMATION ASSURANCE AGREEMENT**

Dated

2015

THE POLICE AND CRIME COMMISSIONER FOR LEICESTERSHIRE  
THE POLICE AND CRIME COMMISSIONER FOR NOTTINGHAMSHIRE  
THE POLICE AND CRIME COMMISSIONER FOR NORTHAMPTONSHIRE  
THE POLICE AND CRIME COMMISSIONER FOR DERBYSHIRE  
THE POLICE AND CRIME COMMISSIONER FOR LINCOLNSHIRE  
THE CHIEF CONSTABLE OF LEICESTERSHIRE POLICE  
THE CHIEF CONSTABLE OF NOTTINGHAMSHIRE POLICE  
THE CHIEF CONSTABLE OF NORTHAMPTONSHIRE POLICE  
THE CHIEF CONSTABLE OF DERBYSHIRE CONSTABULARY  
THE CHIEF CONSTABLE OF LINCOLNSHIRE POLICE

## CONTENTS

1.	INTRODUCTION AND LEGAL CONTEXT .....	3
2.	DEFINITIONS AND INTERPRETATIONS .....	3
3.	COLLABORATIONS .....	5
4.	THE RIAG AND RIAG MEETINGS .....	6
5.	THE RIAG'S TERMS OF REFERENCE AND AIMS .....	7
6.	THE CHAIR'S RESPONSIBILITIES .....	7
7.	PUBLICITY .....	8
8.	PUBLIC INTEREST DISCLOSURE .....	8
9.	LIABILITIES .....	8
10.	NOTICES .....	8
11.	REVIEW AND VARIATION OF AGREEMENT .....	9
12.	WITHDRAWAL AND TERMINATION .....	9
13.	CONSEQUENCES OF TERMINATION .....	9
14.	DISPUTES AND ARBITRATION .....	9
15.	ASSIGNMENT & SUCCESSORS TO THE PCC .....	10
16.	ILLEGAL/UNENFORCEABLE PROVISIONS .....	10
17.	WAIVER OF RIGHTS .....	10
18.	ENTIRE AGREEMENT .....	10
19.	FURTHER ASSURANCES .....	10
20.	COUNTERPARTS .....	10
21.	THIRD PARTIES .....	10
22.	GOVERNING LAW .....	10
	SCHEDULE 1 .....	11
	PROJECT PROTOCOL .....	11
	SCHEDULE 2 .....	12
	FLOWCHART OF REGIONAL INFORMATION ASSURANCE PROCESS .....	12
	SCHEDULE 3 .....	13
	REGIONAL POLICIES .....	13
	SCHEDULE 4 .....	14
	ADDRESSES FOR SERVICE .....	14
	SCHEDULE 5 .....	15
	INFORMATION MANAGEMENT .....	15
	SCHEDULE 6 .....	22
	TEMPLATE COLLABORATION APPENDIX .....	22
	SCHEDULE 7 .....	24
	FINAL SPECIFIC COLLABORATION APPENDICES .....	24

THIS AGREEMENT is made on

2015

BETWEEN the following parties (each a “Party” and together the “Parties”):

- (1) **The Police and Crime Commissioner for Leicestershire** of Force Headquarters, St. Johns, Enderby, Leicestershire, LE19 2BX and **the Chief Constable of Leicestershire Police** of Force Headquarters, St. Johns, Enderby, Leicestershire, LE19 2BX (collectively known as “**Leicestershire Police**”); and
- (2) **The Police and Crime Commissioner for Nottinghamshire** of Arnot Hill House, Arnot Hill Park, Arnold, Nottingham, NG5 6LU and **the Chief Constable of Nottinghamshire Police** of Force Headquarters, Sherwood Lodge, Arnold, NG5 8PP (collectively known as “**Nottinghamshire Police**”); and
- (3) **The Police and Crime Commissioner for Derbyshire** of Force Headquarters, Derbyshire Constabulary, Butterley Hall, Ripley, Derby DE5 3RS and **the Chief Constable of Derbyshire Constabulary** of Force Headquarters, Derbyshire Constabulary, Butterley Hall, Ripley, Derby DE5 3RS (collectively known as “**Derbyshire Constabulary**”); and
- (4) **The Police and Crime Commissioner for Northamptonshire** of Wootton Hall, Northamptonshire NN4 0JQ and **the Chief Constable of Northamptonshire Police** of Wootton Hall, Northamptonshire NN4 0JQ (collectively known as “**Northamptonshire Police**”); and
- (5) **The Police and Crime Commissioner for Lincolnshire** of Police Headquarters, Deepdale Lane, Nettleham, near Lincoln LN2 2LT and **the Chief Constable of Lincolnshire Police** of Police Headquarters, Deepdale Lane, Nettleham, near Lincoln LN2 2LT (collectively known as “**Lincolnshire Police**”).

## 1. Introduction and Legal Context

- 1.1. The Parties are (and shall be) parties to a number of Collaborations, under the terms of which Police Data (which may include Personal Data) may be used, accessed, hosted, processed and/or shared between some or all of the Parties.
- 1.2. This Agreement sets out the terms and conditions under which Police Data may be shared between the Parties and under which Personal Data will be processed by the Data Processor together with the general responsibilities of each Data Controller and Data Processor.
- 1.3. This Agreement will take effect from the Effective Date and will continue in force until terminated in accordance with **clause 12**.

## 2. Definitions and Interpretations

- 2.1. In this Agreement except where a different interpretation is clear from, or necessary in the context, the following terms shall have the following meanings:
  - 2.1.1. “**Agreement**” means this document, including its clauses and schedules, as amended from time to time in accordance with **clause 11**;
  - 2.1.2. “**Aims**” means the aims of the RIAG as identified by the Parties and set out in **clause 5**;
  - 2.1.3. “**BCDR Plan**” means the Business Continuity and Disaster Recovery Plan attached to the Collaboration Appendix or, failing that, the Business Continuity and Disaster Recovery Plan of the Data Processor for that Collaboration;
  - 2.1.4. “**Business Day**” means any day other than a Saturday, Sunday or public holiday in England;
  - 2.1.5. “**Chief Constables**” means the Chief Constables who are Parties to this Agreement and “**Chief Constable**” means any one of them;
  - 2.1.6. “**Collaboration**” means a collaboration or provision of mutual aid or any other cooperation between two or more PCCs, or two or more Chief Constables and two or more PCCs (whether pursuant to section 22A of the Police Act 1996 or otherwise) which involves shared information technology, communication systems, information assurance, information management and/or the hosting, sharing, using, processing and/or shared access to Police Data;
  - 2.1.7. “**Collaboration Agreement**” means an agreement setting out the terms and conditions of a Collaboration entered into between two or more PCCs, or two or more Chief Constables and two or more PCCs, under section 22A of the Police Act 1996;
  - 2.1.8. “**Collaboration Appendix**” means the appendix for a Collaboration, substantially in the form of the Template Collaboration Appendix;

- 2.1.9. **"Contract"** means this Agreement and/or any Collaboration Agreement and/or any Collaboration Appendix, as the context requires;
- 2.1.10. **"Contracting Authority"** means any contracting authority as defined in Regulation 5(2) of the Public Contracts (Works, Services and Supply) (Amendment) Regulations 2000, other than the Parties;
- 2.1.11. **"Data Controller"** has the meaning given to it in the Data Protection Act 1998 and shall be the Party(ies) identified as such in the relevant Collaboration Appendix;
- 2.1.12. **"Data Processor"** has the meaning given to it in the Data Protection Act 1998 and shall be the Party identified as such in the relevant Collaboration Appendix;
- 2.1.13. **"Data Protection Law"** means the Data Protection Act 1998, the Data Protection Directive (95/46/EC), the Regulation of Investigatory Powers Act 2000, the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 (SI 2000/2699), the Electronic Communications Data Protection Directive (2002/58/EC), the Privacy and Electronic Communications (EC Directive) Regulations 2003 (SI 2426/2003), the Protection of Freedoms Act 2012 and all applicable laws and regulations relating to the processing of Personal Data and privacy, including where applicable the guidance and codes of practice issued by the Information Commissioner;
- 2.1.14. **"Designated Police Manager"** means the Chief Constable or such other senior post holder responsible for the relevant Collaboration, on behalf of the Data Processor or Data Controller(s), as identified in the relevant Collaboration Appendix;
- 2.1.15. **"Effective Date"** means the date of this Agreement;
- 2.1.16. **"Environmental Information Regulations"** means the Environmental Information Regulations 2004 together with any guidance and/or codes of practice issued by the Information Commissioner or relevant Regulatory Body in relation to such regulations;
- 2.1.17. **"FOIA"** means the Freedom of Information Act 2000;
- 2.1.18. **"Government Protective Marking Scheme"** means a scheme for the classification of information pursuant to the Cabinet Office's protective marking scheme or the equivalent classification under the Cabinet Offices' new Government Security Classification Scheme;
- 2.1.19. **"Information"** has the meaning given under section 84 of the FOIA;
- 2.1.20. **"Intellectual Property"** means any patents, trade marks, service marks, registered designs, copyrights, database rights, design rights, know-how, confidential information, applications for any of the above, and any similar right recognised from time to time in any jurisdiction, together with all rights of action in relation to the infringement of any of the above;
- 2.1.21. **"ISO"** means Information Security Officer;
- 2.1.22. **"IT System"** means the computing environment (consisting of hardware, software and/or telecommunications networks or equipment) used by or on behalf of the Data Processor or any Data Controller, or any of its employees, agents, consultants and contractors, to host, access or otherwise process the Police Data and, where applicable, identified in the Collaboration Appendix;
- 2.1.23. **"Law"** means any applicable law, statute, by-law, regulation, order, regulatory policy, guidance or industry code, rule of court or directive or requirement of any Regulatory Body, delegated or subordinate legislation or notice of any Regulatory Body;
- 2.1.24. **"Malicious Software"** means any software program or code intended to destroy, interfere with, corrupt or cause undesired effects on program files, data, executable code or application software macros, whether or not its operation is immediate or delayed, and whether the malicious software is introduced wilfully, negligently or without knowledge of its existence;
- 2.1.25. **"MOPI"** means the Code of Practice for the Management of Police Information (2005);
- 2.1.26. **"PCCs"** means the Police and Crime Commissioners who are Parties to this Agreement and any successor bodies of those PCCs and **"PCC"** means any one of them;
- 2.1.27. **"Personal Data"**, **"Sensitive Personal Data"**, **"Data Subject"**, **"Subject Access"**, **"Information Commissioner"**, **"process"** and **"processing"** will have the meanings given to those terms by the Data Protection Act 1998;
- 2.1.28. **"Police Data"** means any data (including Personal Data) text, drawings, diagrams, images or sounds (together with any database made up of any of these) which are embodied in any



electronic, magnetic, optical or tangible media, and which are provided by the Data Controller(s) to the Data Processor and/or to be shared with or accessed by another Party pursuant to the relevant Collaboration;

- 2.1.29. **"Project Protocol"** means the protocol set out in **Schedule 1**;
  - 2.1.30. **"Purpose"** means the purpose for which the Police Data is processed and/or shared as identified in the relevant Collaboration Appendix, or if no Collaboration Appendix exists the purpose agreed by the parties to the Collaboration;
  - 2.1.31. **"Regional Policies"** means the agreed regional policies and procedures listed in **Schedule 3** as may be updated, modified or replaced from time to time by the Parties;
  - 2.1.32. **"Regulatory Bodies"** means those government departments and regulatory, statutory and other entities, committees, ombudsmen and bodies which, whether under statute, rules, regulations, codes of practice or otherwise, are entitled to regulate, investigate, or influence the matters dealt with in the Contract or any other affairs of the Parties and **"Regulatory Body"** shall be construed accordingly;
  - 2.1.33. **"Request for Information"** means a request for information or an apparent request under the Code of Practice on Access to Government Information, FOIA or the Environmental Information Regulations;
  - 2.1.34. **"RIAG"** means the Regional Information Assurance Group;
  - 2.1.35. **"RMADS"** means the Risk Management Accreditation Document Set for the relevant Collaboration, agreed in accordance with the Project Protocol;
  - 2.1.36. **"Senior Information Risk Owner"** or **"SIRO"** means the person identified as such for each Party in the relevant Collaboration Appendix or, if no Collaboration Appendix exists, the Deputy Chief Constable;
  - 2.1.37. **"Shared Services Senior Information Risk Owner"** or **"SSSIRO"** means the person identified as such in the Collaboration Appendix or, if no Collaboration Appendix exists, the SIRO of the police force hosting the Police Data; and
  - 2.1.38. **"Template Collaboration Appendix"** means the pro forma appendix to be used for each Collaboration as set out in **Schedule 6**.
- 2.2. In this Agreement unless the context requires otherwise:
- 2.2.1. words importing the singular shall include the plural and vice versa;
  - 2.2.2. words importing any particular gender shall include all other genders;
  - 2.2.3. references to persons shall include bodies of persons whether corporate or incorporate;
  - 2.2.4. words importing the whole shall be treated as including a reference to any part of the whole;
  - 2.2.5. any reference in this Agreement to any statute or statutory provision shall be construed as referring to that statute or statutory provision as it may from time to time be amended modified extended re-enacted or replaced (whether before or after the Effective Date) and including all subordinate legislation from time to time made under it;
  - 2.2.6. references in this Agreement to any clauses and Schedules are to the clauses and Schedules to this Agreement except where otherwise expressly stated; and
  - 2.2.7. headings are used in this Agreement for the convenience of the Parties only and shall not be incorporated into this Agreement and shall not be deemed to be any indication of the meaning of the clauses or Schedules to which they relate.
3. **Collaborations**
- 3.1. It is intended that each Collaboration shall be governed by the terms of this Agreement.
  - 3.2. Subject to **clause 3.3**, the Parties agree that they shall adopt and follow the Project Protocol when considering any Collaboration or proposed Collaboration including agreeing and finalising the terms of the relevant Collaboration Agreement.
  - 3.3. The Parties agree that (as far as possible) each Collaboration shall have a Collaboration Appendix setting out at least the following in respect of that Collaboration:
    - 3.3.1. the purpose of the Collaboration and reason why the Police Data is required to be shared to meet that purpose;

- 3.3.2. which Parties will be a party to the Collaboration;
  - 3.3.3. the types of Police Data to be shared (including security level in line with the Government Protective Marking Scheme) and with whom;
  - 3.3.4. the basis for sharing the Police Data;
  - 3.3.5. identifying any Personal Data within the Police Data and whether it includes Sensitive Personal Data;
  - 3.3.6. the identity of the Data Processor;
  - 3.3.7. the identity of the Data Controller(s);
  - 3.3.8. the point at which the identity of any Data Controller may change (and the impact (if any) such change will have on the responsibilities of each Data Controller);
  - 3.3.9. the specific responsibilities of each Data Controller, should these differ from the terms set out in this Agreement;
  - 3.3.10. overall responsibility for providing access to shared Police Data and responding to Subject Access requests, should this differ from the terms set out in this Agreement;
  - 3.3.11. technical and organisational security arrangements, should these differ from the terms set out in this Agreement.
- 3.4. A copy of each finalised and signed Collaboration Appendix shall be attached to this Agreement at **Schedule 7**.
- 3.5. In the event of any conflict between the provisions of **Schedule 5** and/or the contents of a Collaboration Appendix and/or any Collaboration Agreement, the following order of precedence shall apply:
- 3.5.1. the provisions of the Collaboration Appendix; then
  - 3.5.2. the provisions of **Schedule 5**; then
  - 3.5.3. the Collaboration Agreement.
- 3.6. In implementing a Collaboration and carrying out its obligations in respect of the Collaboration (including its obligations under any Collaboration Agreement), each Party to a Collaboration shall comply with:
- 3.6.1. the Regional Policies; and
  - 3.6.2. the provisions on Information Management as set out at **Schedule 5**,
  - 3.6.3. which shall form part of and be deemed incorporated into the terms of the relevant Collaboration (including any Collaboration Agreement).
- 3.7. In the event of any conflict between the Regional Policies, the provisions of **Schedule 5** and/or any policy of a Data Processor or a home police force and/or any Collaboration Agreement, the following order of precedence shall apply:
- 3.7.1. the provisions of **Schedule 5**; then
  - 3.7.2. the Collaboration Agreement; then
  - 3.7.3. the Regional Policies; then
  - 3.7.4. the policy of the Data Processor.
- 3.8. It is the Parties' intention that any Collaboration Agreement will set out all other relevant terms for that Collaboration including non-IT policies and procedures and provisions relating to staff, premises, assets, vehicles, liability and insurance.
- 4. The RIAG and RIAG Meetings**
- 4.1. The RIAG will be chaired by the Nottinghamshire Police Deputy Chief Constable or such other person appointed by the Chief Constables or agreed by their nominated representatives.
- 4.2. Each RIAG will consist of:
- 4.2.1. the person appointed as chairperson under **clause 4.1** (the "Chair");
  - 4.2.2. the Information Manager from each force a Party to this Agreement; and

4.2.3. the ISO from each force a Party to this Agreement.

- 4.3. The RIAG may, where it considers it necessary or desirable, invite any additional individuals to a meeting of the RIAG to assist it in performing its functions under this Agreement.
- 4.4. All members of the RIAG or invitees to an RIAG meeting will be vetted as appropriate.
- 4.5. Any member of the RIAG may participate in RIAG meetings by tele-conference, video-conference, or any other technology that enables everyone participating in the meeting to communicate interactively and simultaneously with each other.
- 4.6. The quorum for a meeting of the RIAG will be one representative of each force a Party to this Agreement present in person, or by tele-conference, video-conference, or other technology mentioned above.
- 4.7. In the absence of the Chair, the RIAG may appoint another person from among its members to act as Chair for meetings of the RIAG from time to time.
- 4.8. The Parties will ensure that the RIAG meets at least every (three) months at venues and times to be agreed by the Parties.
- 4.9. Meetings of the RIAG will be convened with at least 14 days written notice provided to the RIAG members in advance. That notice must include an agenda. Minutes of the meetings of the RIAG will be prepared by the Regional Project Management Officer or, in their absence, the Chair's PA and shall be sent to each of the Parties within fourteen days after each meeting.
- 4.10. Each RIAG member will through its representative, or alternate, have a single vote on the RIAG. Decisions will be taken by a simple majority.
- 4.11. Save where the matter would fall within the responsibilities of the PCCs, the Chair may at his/her sole discretion determine that any decision before the RIAG should be determined by the Chief Constables or their nominated delegates.

## **5. The RIAG's Terms of Reference and Aims**

### **5.1. The RIAG will:**

- 5.1.1. ensure RIAG's compliance with legal requirements and national standards;
- 5.1.2. monitor the ethical standards within RIAG;
- 5.1.3. support the continued development of the long standing and effective collaboration across the Parties by ensuring RIAG's proper function and integration with other collaborative work streams;
- 5.1.4. approve policies for the RIAG;
- 5.1.5. consider, review and, if deemed appropriate, approve the addition of new Collaborations to be governed by the terms of this Agreement;
- 5.1.6. prioritise Collaboration workload to strike a balance between local, regional and national activities;
- 5.1.7. champion the aims of regional collaboration convergence within the Parties;
- 5.1.8. provide an executive link between the governance of local police force change projects and regional projects; and
- 5.1.9. review and, if appropriate, update these Aims at least every year.

## **6. The Chair's Responsibilities**

### **6.1. The Chair shall be responsible for:**

- 6.1.1. the organisation, direction and management of the RIAG;
- 6.1.2. the formulation (in consultation with other RIAG members where necessary) of policy, procedure and guidance for the RIAG;
- 6.1.3. the determination (in consultation with other RIAG members) of RIAG's operational and management activities, and its other activities;
- 6.1.4. reporting to the Deputy Chief Constables on the activities of the RIAG.

**7. Publicity****7.1. No Party shall:**

- 7.1.1. take steps to publicise the existence of this Agreement or any operation or investigation undertaken pursuant to any authorisation under this Agreement or a Collaboration Agreement without the prior written approval of the other Parties; or
- 7.1.2. use any other Party's name, logo or brand in any promotion or marketing or announcement of orders without the prior written approval of the other Party; or
- 7.1.3. issue any press release or other public document, or make any public statement, containing or otherwise disclose to any person who is not a party, information which relates to or is connected with or arises out of this Agreement or the matters contained in it (including any Collaboration), without the prior written approval of the other Parties. The Parties shall in any event consult together upon the form of any such press release, document, or statement as and when such releases are required.

7.2. Each Party will notify the relevant Party or Parties as soon as reasonably practicable of any fact or occurrence of which it is or becomes aware relating to another Party (or Parties) that could, in the reasonable opinion of that Party, be expected to cause adverse publicity to the another Party (or Parties) in relation to this Agreement or any Collaboration.

7.3. Each Party will be entitled to publicise this Agreement and any Collaboration Agreement in accordance with any legal obligation on it, including:

- 7.3.1. any examination of this Agreement or the relevant Collaboration Agreement by an external auditor or otherwise;
- 7.3.2. pursuant to the PCCs' statutory obligations under the Elected Local Policing Bodies (Specified Information) Order 2011.

**8. Public Interest Disclosure**

8.1. The Parties acknowledge and agree that for the purposes of the legal protection against victimisation and dismissal provided under the Public Interest Disclosure Act 1998 ("PIDA") for individuals who disclose information so as to expose malpractice and matters of similar concern (known as "whistle blowers"), police officers and police staff shall be entitled to report such "whistle blowing" matters back to their home police force and it is their home police force who shall be obliged to give such legal protection pursuant to PIDA.

**9. Liabilities**

9.1. The Parties acknowledge and agree that in the absence of a Collaboration Agreement or Collaboration Appendix or other agreement stating the contrary, the Parties to a Collaboration shall be jointly and severally liable for any and all liabilities that may arise in relation to that Collaboration.

**10. Notices**

10.1. Any notice to be given under this Agreement must be in writing, may be delivered to the other Party or Parties by any of the methods set out in the left hand column below and will be deemed to be received on the corresponding day set out in the right hand column.

Method of service	Deemed day of receipt
By hand or courier	the day of delivery
By pre-paid first class post	the second Business Day after posting
By recorded delivery post	the next Business Day after posting
By fax (provided the sender's fax machine confirms complete and error-free transmission of that notice to the correct fax number)	the next Business Day after sending or, if sent before 16.00, on the Business Day it was sent
By email (provided the recipient confirms complete and error-free transmission of that notice to the correct email address)	the next Business Day after sending or, if sent before 16.00, on the Business Day it was sent

10.2. The Parties' respective representatives for the receipt of notices are, until changed by notice given in accordance with this clause 10, the Chief Constable of each Party and the Chief Executive of each

PCC (the addresses for service are set out in **Schedule 4**).

#### **11. Review and Variation of Agreement**

- 11.1. The Parties shall review this Agreement (including the Aims, the Project Protocol and the Regional Policies) on an annual basis and the Parties may make any amendments necessary by agreement in writing subject to **clause 11.2**.
- 11.2. A variation agreed by the Parties which amounts to a material variation (other than a change to the Aims, the Project Protocol or the Regional Policies) will constitute the termination of this Agreement and give rise to the requirement for a new agreement. Where amendments are made, they will be subject to any relevant approvals/consultations set out in the Police Act 1996 (as amended by the Police Reform and Social Responsibility Act 2011) (the "Act").

#### **12. Withdrawal and Termination**

- 12.1. The Parties agree that this Agreement may be terminated at any time by all the Parties.
- 12.2. The Parties acknowledge that the nature of the RIAG is such that there is a significant inter-dependency between the obligations of the PCCs and those of the Chief Constables under this Agreement. Subject to any obligations or requirements of the Act including but not limited to any direction of the Secretary of State the Parties agree that:
- 12.2.1. if a Chief Constable or PCC wishes to withdraw from this Agreement then their respective Chief Constable or PCC will also withdraw from this Agreement;
- 12.2.2. if a Chief Constable and PCC wish to withdraw from this Agreement pursuant to **clause 12.2.1** they may withdraw by giving not less than one month's written notice to the RIAG, the Chief Constables and the PCCs.
- 12.3. The Secretary of State may terminate this Agreement in whole or in part with immediate effect or at the end of a specified period.

#### **13. Consequences of Termination**

- 13.1. In the event of termination of this Agreement as a whole in accordance with **clause 12.1** and no subsequent agreement being formed for RIAG:
- 13.1.1. the Chief Constables and PCCs will use their best endeavours to minimise the effect on any outstanding police operation, investigation or prosecution by providing reasonable and proportionate assistance to the Chief Constable assuming responsibility;
- 13.1.2. all Intellectual Property developed by the RIAG will be vested jointly in the PCCs.
- 13.2. The termination of this Agreement or withdrawal by a Party from this Agreement, shall not affect any existing Collaborations or Collaboration Agreements and the Parties shall continue to be bound by the terms of this Agreement for existing Collaborations unless the Parties agree otherwise in writing. However, the Parties acknowledge that the termination of this Agreement or the withdrawal of a Party will necessitate further discussion and agreement in respect of any shared information technology, communication systems, information assurance, information management and/or the hosting, sharing, using, processing and/or shared access to Police Data taking place under the terms of existing and future Collaborations.

#### **14. Disputes and Arbitration**

- 14.1. Any dispute between the Parties arising out of or in connection with this Agreement or its dissolution will in the first instance be referred to a meeting of the Chief Constables and the PCCs for discussion and to attempt to resolve the matter. If the dispute is not resolved at that meeting the dispute shall be referred to a single arbitrator to be agreed upon by the Parties or in default of agreement to be nominated by the President for the time being of the Chartered Institute of Arbitrators in accordance with the Arbitration Act 1996.
- 14.2. Nothing in **clause 14.1** shall restrict at any time while the dispute resolution procedure is in progress, or before it is evoked, the freedom of any Party to commence legal proceedings to preserve a legal right or remedy pending the outcome of the dispute.
- 14.3. If a dispute is referred to arbitration, the disputing Parties will comply with the following provisions:
- 14.3.1. the arbitration will be governed by the provisions of the Arbitration Act 1996 and the London Court of International Arbitration ("LCIA") procedural rules will be applied and are deemed to be incorporated into this Agreement (save that, in the event of any conflict between those rules and this Agreement, this Agreement will prevail);

14.3.2. the decision of the arbitrator will be binding on the disputing Parties (in the absence of any material failure by the arbitrator to comply with the LCIA procedural rules);

14.3.3. the arbitration proceedings will take place in a location to be agreed between the Parties or in default of agreement to be determined by the appointed arbitrator.

**15. Assignment & Successors to the PCC**

15.1. Subject to **clause 15.2** and except by statutory enactment, none of the Parties may assign or transfer this Agreement as a whole, or any of its rights or obligations under it, without first obtaining the written consent of all of the other Parties (such consent not to be unreasonably withheld or delayed).

15.2. Any change in the legal status of any PCC such that it ceases to be a legal entity for the purpose of this Agreement shall not affect the validity of this Agreement. In such circumstances, this Agreement shall bind and inure to the benefit of any successor body to any PCC.

**16. Illegal/unenforceable Provisions**

16.1. If the whole or any part of any provision of this Agreement is void or unenforceable, the other provisions of this Agreement, and the rest of the void or unenforceable provision, will continue in force.

**17. Waiver of rights**

17.1. If a Party fails to enforce or delays in enforcing an obligation of any other Party, or fails to exercise or delays in exercising a right under this Agreement, that failure or delay will not affect its right to enforce that obligation or constitute a waiver of that right. Any waiver by a Party of any provision of this Agreement will not, unless expressly stated to the contrary, constitute a waiver of that provision on a future occasion.

**18. Entire Agreement**

18.1. This Agreement (together with the documents referred to in it) constitutes the entire agreement between the Parties relating to its subject matter. Each Party acknowledges that it has not entered into this Agreement on the basis of any warranty, representation, statement, agreement or undertaking except those expressly set out in this Agreement. Each Party waives any claim for breach of this Agreement, or any right to rescind this Agreement in respect of any representation which is not an express provision of this Agreement. However, this **clause 18** does not exclude any liability which any Party may have to any other (or any right which any Party may have to rescind this Agreement) in respect of any fraudulent misrepresentation or fraudulent concealment prior to the execution of this Agreement.

**19. Further Assurances**

19.1. Each Party shall, at the request of any other Party, provide all reasonable support and assistance which may be necessary to give effect to this Agreement or any of the provisions hereunder.

19.2. Without prejudice to the generality of **clause 19.1**, each Party will take any action and execute any document reasonably requested by any other Party to give effect to any of its rights under this Agreement.

**20. Counterparts**

20.1. This Agreement may be executed in any number of counterparts, each of which, when signed shall be an original, and all the counterparts together shall constitute one and the same instrument.

**21. Third Parties**

21.1. Except as otherwise provided by the Act or other statutory enactment, no one except a Party to this Agreement has any right to prevent the amendment of this Agreement or its termination, and no one except a Party to this Agreement may enforce this Agreement.

**22. Governing Law**

22.1. This Agreement is governed by, and is to be construed in accordance with, English Law. Subject to **clause 14**, the Parties agree that the English Courts will have exclusive jurisdiction to deal with any dispute which has arisen or may arise out of or in connection with this Agreement.

## **SCHEDULE 1**

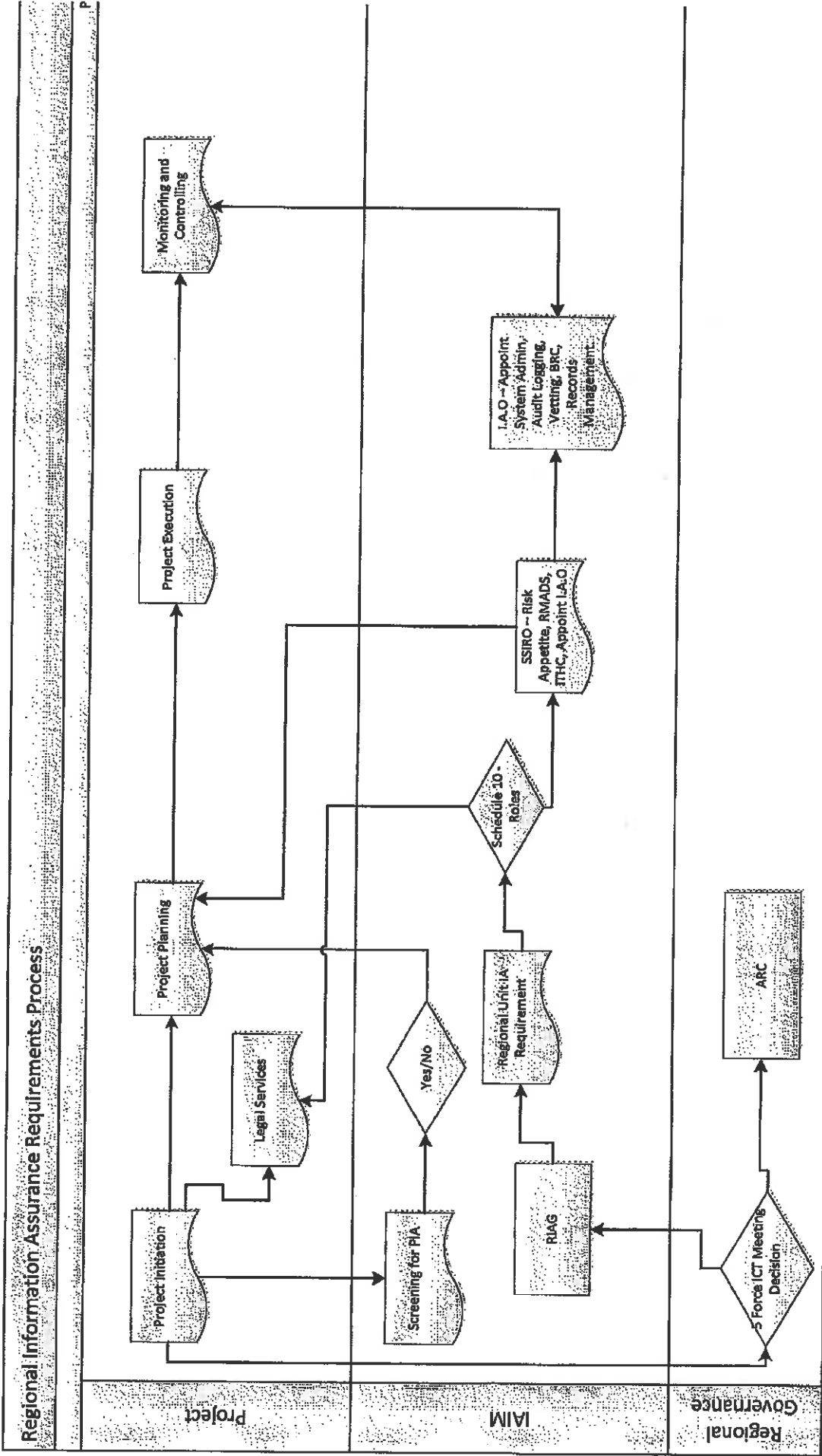
### **Project Protocol**

For each Collaboration, the Parties to that Collaboration shall, in conjunction and consultation with the RIAG:

- agree the Collaboration's governance framework and decision making process;
- agree and put in place any additional policies required for the Collaboration (eg shared services security policy);
- agree appropriate service levels for the provision of any IT support services provided as part of (or required in relation to) the Collaboration;
- undertake a risk assessment for the Collaboration and agree the Collaboration's risk appetite statement;
- sign and complete RMADS for the Collaboration;
- undertake a privacy impact assessment;
- appoint and identify (and define the roles and responsibilities of) the following (where appropriate) for the Collaboration:
  - SIRO;
  - Designated Police Manager;
  - ISO
  - Shared Services SIRO;
  - Shared Services ITSO;
  - Shared Services Lead Accreditor;
  - Shared Services Security and Information Risk Advisor;
  - Information Asset Owner;
  - System Administrator.

The flow-chart at **Schedule 2** shows how the RIAG will interact with the project lead for the relevant Collaboration.

SCHEDULE 2  
Flowchart of Regional Information Assurance Process





**SCHEDULE 3**  
**Regional Policies**

As at the date of this Agreement, there are none.

**SCHEDULE 4**  
**Addresses for Service**

**The Police and Crime Commissioner for Leicestershire:** Force Headquarters, St Johns, Enderby, Leicestershire, LE19 2BX

**The Police and Crime Commissioner for Northamptonshire:** Wootton Hall, Northampton, NN4 0JQ

**The Police and Crime Commissioner for Nottinghamshire:** Arnot Hill House, Arnot Hill Park, Arnold, Nottingham, NG5 6LU

**The Police and Crime Commissioner for Derbyshire:** Force Headquarters, Butterley Hall, Ripley, Derbyshire, DE5 3RS

**The Police and Crime Commissioner for Lincolnshire:** Police Headquarters, Deepdale Lane, Nettleham, Lincoln, Lincolnshire, LN2 2LT

**Chief Constable of Leicestershire Police:** Force Headquarters, St Johns, Enderby, Leicester, LE19 2BX

**Chief Constable of Northamptonshire Police:** Force Headquarters, Wootton Hall, Northampton, NN4 0JQ

**Chief Constable of Nottinghamshire Police:** Force Headquarters, Sherwood Lodge, Arnold, Nottingham, NG5 8PP

**Chief Constable of Derbyshire Constabulary:** Force Headquarters, Butterley Hall, Ripley, Derbyshire, DE5 3RS

**Chief Constable of Lincolnshire Police:** Police Headquarters, Deepdale Lane, Nettleham, Lincoln, Lincolnshire, LN2 2LT

## **SCHEDULE 5**

### **Information Management**

**(including FOIA, Confidentiality, Data Protection, Data Security and Risk Management)**

#### **1. Freedom of Information**

- 1.1. Each Party acknowledge that the Parties are subject to the requirements of the FOIA and the Environmental Information Regulations and will assist and co-operate with the other Parties to enable each Party to comply with its Information disclosure obligations.
- 1.2. Each Party will (and will ensure that the RIAG will):
  - 1.2.1. transfer to the relevant Party's Data Protection Officer all Requests for Information relating to that Party that they receive as soon as practicable and in any event within 2 Business Days of receiving a Request for Information;
  - 1.2.2. provide the relevant Party with a copy of all Information in their possession or power in the form that the relevant Party requires within 5 Business Days of the Party's request;
  - 1.2.3. provide all necessary assistance as reasonably requested by the relevant Party to enable the relevant Party to respond to the Request for Information within the time for compliance set out in section 10 of the FOIA or regulation 5 of the Environmental Information Regulations; and
  - 1.2.4. not respond directly to a Request for Information relating to any other Party(ies) without first consulting with the other Party(ies).
- 1.3. Notwithstanding any other provision in the Contract, each Party will be responsible for determining in its absolute discretion whether any Information is exempt from disclosure in accordance with the provisions of the FOIA or the Environmental Information Regulations.
- 1.4. The Parties acknowledge that (notwithstanding the provisions of this **paragraph 1**) each Party may, acting in accordance with the Department of Constitutional Affairs' Code of Practice on the Discharge of the Functions of Public Authorities under Part 1 of the Freedom of Information Act 2000 ("**Code**"), be obliged under the FOIA or the Environmental Information Regulations to disclose Information concerning the other Party:
  - 1.4.1. in certain circumstances without consulting the other Party; or
  - 1.4.2. following consultation with the other Party and having taken its views into account,provided always that where **paragraph 1.4.1** applies the Party will, in accordance with any recommendations of the Code, take reasonable steps, where appropriate, to give the other Party advanced notice or, failing that, to draw the disclosure to the other Party's attention after any such disclosure.

#### **2. Confidentiality**

- 2.1. Except to the extent set out in this **paragraph 2** or where disclosure is expressly permitted elsewhere in the Contract, each Party (the "**Receiving Party**") will:
  - 2.1.1. treat the Confidential Information of another Party (the "**Disclosing Party**") as confidential and safeguard it accordingly; and
  - 2.1.2. not disclose the Disclosing Party's Confidential Information to any other person without the Disclosing Party's prior written consent; and
  - 2.1.3. not use any of the Disclosing Party's Confidential Information otherwise than for the purposes of the Contract.
- 2.2. **Paragraph 2.1** will not apply to the extent that:
  - 2.2.1. such disclosure is a requirement of Law placed upon the Receiving Party making the disclosure (including any requirements for disclosure under the FOIA or the Environmental Information Regulations pursuant to **paragraph 1**) or the Receiving Party if required to do so by a court of competent jurisdiction or by any Regulatory Body with jurisdiction over the Receiving Party provided that the Receiving Party will
    - 2.2.1.1. not make any disclosure without first consulting with the Disclosing Party; and
    - 2.2.1.2. only copy or disseminate Confidential Information to third parties in accordance with

- and to the extent of the relevant Law; or
- 2.2.2. such disclosure is in accordance with the relevant Contract; or
- 2.2.3. such disclosure is made by a Data Processor to enable its employees or a third party supplier to provide maintenance services provided that such services shall be carried out in accordance with the Regional Policies and/or the Data Processor's IT Policies (as appropriate) and the employees or third parties carrying out the maintenance services shall be closely supervised by a member of the Data Processor's IT department at all times; or
- 2.2.4. such information was:
  - 2.2.4.1. in the possession of the Receiving Party making the disclosure without obligation of confidentiality prior to its disclosure by the Disclosing Party; or
  - 2.2.4.2. obtained from a third party without obligation of confidentiality; or
  - 2.2.4.3. already in the public domain at the time of disclosure otherwise than by a breach of the Contract (including the provisions of this **Schedule 5**); or
  - 2.2.4.4. independently developed without access to the Disclosing Party's Confidential Information.
- 2.3. Each Receiving Party may only disclose Confidential Information to its personnel (including its consultants, contractors or other person engaged by the Receiving Party) who are directly involved in the operation of the Contract or the Collaboration (including any personnel providing maintenance services in accordance with **paragraph 2.2.3**) and who need to know such information, and will ensure that such personnel are aware of and will comply with these obligations as to confidentiality. In the event that any default, act or omission of any of the Receiving Party's personnel causes or contributes (or could cause or contribute) to the Receiving Party breaching its obligations as to confidentiality under or in connection with the Contract or the Collaboration:
  - 2.3.1. the relevant Receiving Party will take such action as may be appropriate in the circumstances, including the use of disciplinary procedures in serious cases;
  - 2.3.2. to the fullest extent permitted by its own obligations of confidentiality to any of the Receiving Party's personnel, the relevant Receiving Party will provide such evidence to the Disclosing Party as the Disclosing Party may reasonably require (though not so as to risk compromising or prejudicing the case) to demonstrate that the Receiving Party is taking appropriate steps to comply with this **paragraph 2**, including:
    - 2.3.2.1. copies of any written communications to and/or from the Receiving Party's personnel; and
    - 2.3.2.2. any minutes of meetings and any other records which provide an audit trail of any discussions or exchanges with the Receiving Party's personnel in connection with obligations as to confidentiality.
- 2.4. Nothing in the Contract will prevent any Receiving Party from disclosing the Disclosing Party's Confidential Information:
  - 2.4.1. to any Police and Crime Commissioner, Regulatory Body or to any Contracting Authority (and all Police and Crime Commissioner, Regulatory Bodies or Contracting Authorities receiving such Confidential Information will be entitled to further disclose the Confidential Information to other Police and Crime Commissioners, Regulatory Bodies or other Contracting Authorities on the basis that the information is confidential and is not to be disclosed to a third party that is not part of any Police and Crime Commissioner, Regulatory Body or any Contracting Authority);
  - 2.4.2. for the purpose of the examination and certification of the Receiving Party's accounts; or
  - 2.4.3. for any examination pursuant to section 6(1) of the National Audit Act 1983 of the economy, efficiency and effectiveness with which the Receiving Party has used its resources,
  - 2.4.4. provided that the relevant Receiving Party uses all reasonable endeavours to ensure that the Police and Crime Commissioner, Regulatory Body, Contracting Authority, employee, third party, or sub-contractor to whom the Disclosing Party's Confidential Information is disclosed pursuant to this **paragraph 2.4** is made aware of the Receiving Party's obligations of confidentiality.
- 2.5. Nothing in the Contract will prevent any Party from using any techniques, ideas or know-how gained

during the performance of the Contract or the Collaboration in the course of its normal business to the extent this use does not result in a disclosure of the Disclosing Party's Confidential Information in breach of this **paragraph 2** or an infringement of Intellectual Property.

- 2.6. Each Party will tell the affected Party(ies) immediately if it discovers that any provision of this **paragraph 2** has been breached and will give the affected Party(ies) all reasonable assistance in connection with any proceedings arising from such breach.
- 2.7. The Parties agree that damages may not be an adequate remedy for any breach of this **paragraph 2** by any Party and that the affected Party(ies) will be entitled to obtain any legal and/or equitable relief, including injunction, in the event of any breach of the provisions of this **paragraph 2**.
- 2.8. For the avoidance of doubt nothing in this **paragraph 2** is intended to restrict the PCCs' statutory obligations under the Elected Local Policing Bodies (Specified Information) Order 2011 or any other legislation.
- 2.9. The obligations in this **paragraph 2** will continue without limit in time.

### **3. Data Security**

- 3.1. In accordance with Her Majesty's Government Information Assurance Standards ("HMG IAS") and the ACPO Community Security Policy ("ACPO CSP"), the SSSIRO will ultimately oversee and hold responsibility for information security and information risk management for all business activities undertaken within the terms of the Contract and the Collaboration.
- 3.2. It is recognised that the Data Processor hosts Police Data for and on behalf of the Data Controllers and that some of the Police Data hosted by the Data Processor has been previously protectively marked as 'Restricted' or 'Confidential' by the Data Controller(s) under the Government Protective Marking Scheme.
- 3.3. The Parties acknowledge and agree that the Data Controllers have obligations relating to the security of Police Data in their control under Data Protection Law, MOPI and the ACPO Police Service Information Assurance Strategy.
- 3.4. Each Party acknowledges and agrees that it shall be responsible for the quality of the Police Data that it enters onto the IT System in accordance with MOPI.
- 3.5. The Data Processor, on behalf of the Data Controller(s), during the term of the Contract and any Collaboration, will comply with all relevant obligations:
  - 3.5.1. as detailed in the RMADS submitted by the ISO of the lead force for the Collaboration and approved by the SSSIRO;
  - 3.5.2. in accordance with MOPI, ACPO CSP, HMG IAS and the ACPO Police Service Information Assurance Strategy.
- 3.6. Unless stated otherwise in the Contract, the Data Processor shall:
  - 3.6.1. ensure access to the Police Data is confined to authorised persons only;
  - 3.6.2. take responsibility for preserving the integrity, security and confidentiality of the Police Data and preventing the corruption, unauthorised disclosure or loss of the Police Data;
  - 3.6.3. perform secure back-ups of all the Police Data and shall ensure that up-to-date back-ups are stored off-site in accordance with the BCDR Plan; and
  - 3.6.4. ensure that the IT System is a secure system that complies with the Regional Policies.
- 3.7. If any time, the Data Processor suspects or has reason to believe that the Police Data has or may become corrupted, lost or sufficiently degraded in any way for any reason, then the Data Processor shall notify the relevant Data Controller(s) immediately and inform the relevant Data Controller(s) of the remedial action the Data Processor proposes to take.
- 3.8. If the Police Data is corrupted, lost or sufficiently degraded as a result of the Data Processor's breach of the Contract, the relevant Data Controller(s) may:
  - 3.8.1. require the Data Processor (at the Data Processor's expense) to restore or procure the restoration of the Police Data to the extent and in accordance with the requirements specified in the BCDR Plan and Regional Policies and the Data Processor shall do so as soon as practicable and in any event no later than 3 Business Days after the discovery of the corruption, loss or degradation; or
  - 3.8.2. itself restore or procure the restoration of the Police Data and shall be reimbursed by the Data

Processor any reasonable expenses in doing so, to the extent and in accordance with the requirements specified in the BCDR Plan.

- 3.9. Each Party will, as an enduring obligation throughout the term of the Contract and the Collaboration, use the latest versions of anti-virus definitions and software available from an industry accepted anti-virus software vendor to check for, contain the spread of and minimise the impact of Malicious Software in that Party's systems and/or the IT System.
- 3.10. Notwithstanding paragraph 3.9, if Malicious Software is found on the IT System, the Parties will co-operate to reduce the effect of the Malicious Software and, particularly if Malicious Software causes loss of operational efficiency or loss or corruption of Police Data, assist each other to mitigate any losses.

#### **4. Risk Management**

- 4.1. Each Party to the Collaboration shall comply with the provisions of the BCDR Plan and shall ensure that it is able to implement its obligations under the BCDR Plan at any time.
- 4.2. For each Collaboration, the ISO of the lead force for the Collaboration shall:
  - 4.2.1. assist the project manager for the Collaboration to identify any risks during any on-boarding or implementation stage of the Collaboration and assist the relevant Information Asset Owner(s) once the Collaboration has fully commenced;
  - 4.2.2. ensure that there is a formally documented process for notifying, recording and managing information security incidents. The process will include provision for investigation, escalation relative to risk, media management, notification to the Information Commissioner and formal review of any such incident;
  - 4.2.3. ensure that all Collaboration assets are managed in accordance with the ACPO CSP; to include maintenance of asset registers, licensing, use of removable media, use of encryption and secure disposal at the end of asset life;
  - 4.2.4. ensure that appropriate arrangements are in place to comply with the Government Protective Marking Scheme for all activities undertaken in respect of any Collaboration;
  - 4.2.5. ensure that any and all cryptographic materials are handled and utilised in compliance with HMG IAS 4 or the relevant prevailing standard, with suitably trained and accredited staffing resources in place;
  - 4.2.6. ensure that, where necessary, the IT System is formally 'accredited' in accordance with HMG IAS 1 & 2;
  - 4.2.7. ensure that the procurement and deployment of any new/additional information system utilised for the purposes of the Collaboration is conducted in compliance with ACPO CSP, including the use of formal 'Security Aspects Letters' as necessary.
- 4.3. For each Collaboration, the relevant Information Asset Owner(s) shall:
  - 4.3.1. maintain an information risk register and co-ordinate activity to mitigate identified risks, utilising the collective information security resources of the Parties as necessary and by mutual agreement and report its management of such risks to the SIRO as required;
  - 4.3.2. ensure that there are appropriately documented procedures to manage access to the IT System, proportionate to the risks associated with the IT System and the Collaboration, including any associated personnel security vetting and removal of access, when there is no longer a legitimate business need for that access. This will include any necessary supplementary procedures relating to remote and/or third party access;
  - 4.3.3. ensure that robust arrangements are in place to monitor and audit the use of the IT System, to include appropriate reporting mechanisms and independent verification as necessary;
- 4.4. The SIRO for each Party shall ensure that a robust regime of awareness, training and education is in place and delivered to all of that Party's staff with access to information assets, in accordance with ACPO CSP.
- 4.5. Except as expressly provided otherwise, the Contract does not transfer ownership of or create any licences (implied or otherwise) in any Intellectual Property in any Police Data.
- 4.6. Unless the Collaboration Appendix states otherwise, the Data Processor shall comply with the Data Controller's data retention policy and shall return to the Data Controller any Police Data held by the Data Processor that is no longer required for the purpose for which it was provided.

- 4.7. The Data Processor's Designated Police Manager will be responsible for ensuring the safe subsequent disposal of any archived copies of Police Data that have been created by back-up or recovery procedures carried out by the Data Processor.
- 4.8. Unless the Collaboration Appendix states otherwise, if a Data Controller terminates its involvement or otherwise withdraws from a Collaboration:
  - 4.8.1. a copy of any Police Data owned by that Data Controller (whether solely or jointly with another party to the Collaboration) shall be provided by the Data Processor to the Data Controller in such format and within such timeframe as the Data Controller shall reasonably request; and
  - 4.8.2. any Police Data solely owned by that Data Controller shall be deleted from the IT System and any back-up copies destroyed.
- 5. Data Protection**
- 5.1. Each Party shall
  - 5.1.1. comply with its obligations as Data Controller and/or Data Processor (as appropriate) under any applicable Data Protection Law; and
  - 5.1.2. not, by act or omission, put any other Party in breach of, or jeopardise any registration under, any applicable Data Protection Law.
- 5.2. The Data Processor warrants, undertakes and represents that it shall:
  - 5.2.1. (and will procure that all its agents and sub-contractors will) have in place and implement all appropriate technical and organisational measures to
    - 5.2.1.1. protect against unauthorised or unlawful processing of each Data Controller's Police Data;
    - 5.2.1.2. protect against accidental loss or destruction of, or damage to, each Data Controller's Police Data;
    - 5.2.1.3. deter deliberate compromise or opportunist attack by third parties which would or could compromise each Data Controller's Police Data; and
    - 5.2.1.4. take (and will procure that all its agents and sub-contractors will take) all reasonable steps to ensure the reliability of any staff that may have access to the Data Controller's Police Data;
  - 5.2.2. not copy or store any Police Data on any removable media or any system or media other than the IT System, without the relevant Data Controller's prior written approval;
  - 5.2.3. save where the Collaboration Agreement or Collaboration Appendix states otherwise or where permitted pursuant to **paragraph 5.2.4**, not use the services of any sub-contractors in connection with the processing of the Police Data without the prior written approval of the Data Controller;
  - 5.2.4. ensure that access to the Police Data is limited to those employees or authorised sub-contractors who need access to the Police Data to meet the Data Processor's obligations under the Contract or who carry out maintenance services;
  - 5.2.5. ensure that all employees or authorised sub-contractors with access to Police Data in accordance with this **paragraph 5.2**:
    - 5.2.5.1. are informed of the confidential nature of the Police Data;
    - 5.2.5.2. are appropriately technically qualified;
    - 5.2.5.3. are (or are closely supervised by) authorised members of the Data Processor's IT department; and
    - 5.2.5.4. comply with the Regional Policies and/or the Data Processor's IT Policies (as appropriate Data Processor's IT Policies);
  - 5.2.6. shall (and will procure that all its employees, agents and approved sub-contractors will) act only on the instructions of the Data Controller(s) in relation to the processing of any of the Data Controller's Personal Data and, so that there is no doubt, it is agreed that, save where the Data Processor is also a Data Controller, the Data Processor will only act as a data processor in processing any Personal Data comprised in the Data Controller's Police Data;
  - 5.2.7. only use or process the Data Controller's Police Data for the Purpose or as is necessary to

- perform its obligations under the Contract;
- 5.2.8. it will not generate reports/documents using the Data Controller's Police Data apart from as specified in the Contract or as necessary to carry out protective monitoring of the IT System;
- 5.2.9. it shall allow the Data Controller(s) access on reasonable notice to any of the Data Processor's premises where the Data Controller's Police Data are stored or at which they are accessible to inspect any relevant procedures and/or, at the option of the Data Controller(s), to provide the Data Controller(s) with evidence of the Data Processor's compliance with the provisions of this paragraph 5.
- 5.3. If a Party (the "Recipient") receives a Subject Access request (or other lawful request for Personal Data) relating to Personal Data where it is not the Data Controller, the Recipient will refer the request at the earliest opportunity to the Data Protection Officer or equivalent of the appropriate Data Controller(s) for a response as the Recipient will not be in a position to access or comment on whether there would be harm to the policing purpose through a disclosure.
- 5.4. If a Party (the "Recipient") receives a Subject Access request (or other lawful request for Personal Data) relating to Personal Data where the Recipient is also a Data Controller of that Personal Data with another Party, the Recipient will:
- 5.4.1. promptly inform the other Data Controller(s) about the receipt of any Subject Access request served on the Recipient; and
- 5.4.2. not disclose or release any Personal Data belonging to another Data Controller in response to a Subject Access request served on the Recipient without first consulting with the other Data Controller(s).
- 5.5. The Data Processor will give reasonable assistance as is necessary to the Data Controller(s) in order to enable it/them to comply with such obligations as are imposed on the Data Controller(s) by Data Protection Law in relation to the Personal Data processed by the Data Processor; this assistance includes the obligation to:
- 5.5.1. provide each Data Controller with reasonable assistance in complying with any Subject Access request received by the Data Controller;
- 5.5.2. respond to Information Notices served upon the Data Processor by the Information Commissioner;
- 5.5.3. respond to complaints from Data Subjects;
- 5.5.4. investigate any breach or alleged breach of Data Protection Law by the Data Processor.
- 5.6. The Data Processor will not transfer any of the Data Controller's Personal Data to any country or territory outside the UK other than with the express prior consent of the Data Controller.
- 5.7. The Data Processor will, immediately on demand, fully indemnify each Data Controller and keep each Data Controller fully and effectively indemnified against all costs, claims, demands, expenses (including legal costs and disbursements), losses, actions, proceedings and liabilities of whatsoever nature arising from or incurred by the Data Controller as a result of the loss or destruction of or damage to or unauthorised disclosure of or unauthorised access to the Data Controller's Personal Data in connection with any failure of the Data Processor to comply with the provisions of this paragraph 5 or any Data Protection Law.
- 5.8. The Data Processor will inform the Data Controller promptly of any enquiry, complaint, notice or other communication it receives from any supervisory authority, including the Information Commissioner's Office or any Data Subject, relating to Personal Data processed by it in connection with the Contract or any Collaboration. The Data Processor will provide all necessary assistance to the Data Controller to enable it to respond to such enquiries, complaints, notices or other communications.
- 5.9. Without prejudice to paragraph 5.5.4, in the event of the theft, loss or other unauthorised access to the Data Controller's Personal Data by any person (a "Data Breach"), each Party (other than the Data Controller) will:
- 5.9.1. immediately upon becoming aware of the Data Breach, notify the Data Controller in writing;
- 5.9.2. provide the Data Controller and its advisers with all reasonable assistance in connection with the Data Breach, including:
- 5.9.2.1. co-operating with the Data Controller, the Information Commissioner and any other relevant Regulatory Bodies;



- 5.9.2.2. providing information on the Data Breach to the Data Controller, Information Commissioner and any other relevant Regulatory Bodies;
- 5.9.2.3. investigating the incident and its cause, containing and recovering the compromised Personal Data in compliance with relevant Data Protection Law; and
- 5.9.2.4. co-ordinating with the Data Controller the management of public relations and public statements relating to the Data Breach. For the avoidance of doubt, no Party will make any public statement in relation to a Data Breach except as permitted by **clause 7**.

**SCHEDULE 6**  
**Template Collaboration Appendix**

**Appendix [to the Collaboration Agreement] for (insert)**

Name of Collaboration: (insert title)

Parties to the Collaboration (delete as appropriate)

Derbyshire Constabulary
Leicestershire Police
Lincolnshire Police
Northamptonshire Police
Nottinghamshire Police

**Purpose of the Collaboration:** (insert objectives/aims of the Collaboration and explain why the Police Data set out below is required to be shared between the Parties in order to meet that purpose)

Police Data to be shared

Description of type of Police Data	Security Level under Government Protective Marking Scheme	Categories of Personal Data within this type	Categories of Sensitive Personal Data within this type	Data Processor	Data Controller(s) (and indicate the point(s) at which this status may change)	IT System (ie Location where the Police Data is stored)	Who may access the Police Data

**Information Sharing Process:** (insert basis on which, and process to be followed, for Police Data to be shared/accessed)

**Key Roles**

**Shared Services Senior Information Risk Owner (SSSIRO):** (insert)

**Designated Police Manager** (the senior post holder responsible for the Collaboration) **for each Party:**

Party	Post/Dept
Leicestershire Police	
Derbyshire Police	
Lincolnshire Police	
Northamptonshire Police	
Nottinghamshire Police	

**Shared Services ITSO:** (insert where relevant)

**Shared Services Lead Accreditor:** (insert where relevant)

**Shared Services Security & Information Risk Advisor:** (insert where relevant)

**Information Asset Owner:** (insert where relevant)

**System Administrator:** (insert where relevant)

**ISO:** (insert where relevant)

**Additional Responsibilities or Variations to Regional Information Assurance Agreement**

(insert if any eg additional/specific responsibilities of a Party which differ to the fall-back position set out in the Regional Information Assurance Agreement)

**SCHEDULE 7**  
**Final Specific Collaboration Appendices**  
**[To be attached as agreed & signed]**

Signed by the Parties on the date set out at the beginning of this document.

Signed by

duly authorised to sign for and on behalf of  
POLICE AND CRIME COMMISSIONER FOR  
LEICESTERSHIRE

}   
} P. STOCK


Signed by

duly authorised to sign for and on behalf of  
CHIEF CONSTABLE OF LEICESTERSHIRE  
POLICE

}   
} Simon Wells

Signed by

duly authorised to sign for and on behalf of  
POLICE AND CRIME COMMISSIONER FOR  
NOTTINGHAMSHIRE

}   
} CHRIS EYRE

Signed by

duly authorised to sign for and on behalf of  
CHIEF CONSTABLE OF  
NOTTINGHAMSHIRE POLICE

Signed by

duly authorised to sign for and on behalf of  
POLICE AND CRIME COMMISSIONER FOR  
NORTHAMPTONSHIRE

}   
} John Butts

Signed by

duly authorised to sign for and on behalf of  
CHIEF CONSTABLE OF  
NORTHAMPTONSHIRE POLICE

}   
} Adrian

Signed by

duly authorised to sign for and on behalf of  
POLICE AND CRIME COMMISSIONER FOR  
DERBYSHIRE

}   
} Alan

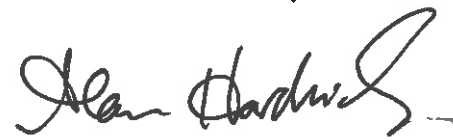
Signed by

duly authorised to sign for and on behalf of  
CHIEF CONSTABLE OF DERBYSHIRE  
CONSTABULARY

}   
} M. L.

Signed by

duly authorised to sign for and on behalf of  
POLICE AND CRIME COMMISSIONER FOR  
LINCOLNSHIRE

}   
} Alan Hardwick

Signed by NEIL RHODES

duly authorised to sign for and on behalf of  
CHIEF CONSTABLE OF LINCOLNSHIRE  
POLICE

}   
} Neil Rhodes

1000

1000

1000