Information Sharing Framework
And
Connection to SafetyNet+

Author:	Performance and Information Team	First issued: 12 November 2018
Owner:	Office of the Police and Crime Commissioner	Version:1.3 Update: 17/01/19

Issuing Authority

Office of the Police and Crime Commissioner.

Readership

It should be read, completed where highlighted and signed by the appropriate authorising signatory in your organisation.

Strategic Overview

The Information Management Board has a strategic overview for the Information Sharing Framework and Connection to SafetyNet+ to ensure appropriate guidelines are in place for partner agencies to operate within to achieve a consistent approach to data quality and maintain the security of the system, and to ensure the platform effectively facilitates multi-agency information sharing.

Further Information

If you require further information or need clarification on any of the contents of this document please contact the OPCC SafetyNet+ System Administrator:
Email: opcc.performance.information@hampshire.pnn.police.uk

Review of this document

The review of this document shall take place annually. Any amendments in this period are to be recorded by the SafetyNet+ System Administrator and issued as an addendum and will be included in the next version.

Purpose

The purpose of this documentation is to provide joining organisations with key information assurances and a structured information sharing framework to safely exchange information with their partners.

Contents

Please sign and return the Connection Agreement and Schedule 3.

History

Version	Issue Date	Reason
1.0	12/11/18	First release of document
1.1	15/11/18	Alternatives provided in the Connection Agreement for organisations without a seal (page 12)
1.2	10/12/18	Improved clarification on required fields to be completed
1.3	17/01/19	Page 2 Readership altered, Page 4 Joining Community Safety Partner address required, Page 11 clause 9.4 reference to November 2004 removed.

Introduction

SafetyNet+ is a secure partnership database for information sharing, joint risk management and problem solving for multi-agency work across Hampshire, Isle of Wight, Portsmouth and Southampton. It has been designed to enable Community Safety Partners, supported by the legitimate legal basis for sharing personal and sensitive data, to work together to protect and safeguard those at most risk and jointly manage those that prevent a threat. It facilitates our joint efforts to reduce crime, promote public safety, and create vibrant and inclusive communities.

Sharing data within SafetyNet+ takes place using two main modules; Integrated Case Management (ICM) and Neighbourhood Management System (NMS). Users enter information onto the system via their browser, which is encrypted in transit between the end user's device and the remote application to the server:

- When submitted to ICM, basic nominal identifiers are visible to all ICM users with further layered restrictions to those with access to the relevant, shared casefiles and activities.
- When submitted to Neighbourhood Management system (NMS) this is then visible by all other users assigned to that neighbourhood area. Specific Police data fields are extracted and published to Police.uk.

SafetyNet+ is managed by the Office of the Police and Crime Commissioner on behalf of community safety partner organisations.

Method of Connection and Requirements

SafetyNet+ is accessible by Authorised Users equipped with an internet connected computer, a web browser (e.g. Internet Explorer), an e-mail client (e.g. Outlook) and a static public facing Internet Protocol Address (an IP Address or range of addresses must be provided upon registration). The application is held on a secure remote server at UniLink Software Ltd, where all work and navigation around the system takes place.

To ensure information is managed securely, all Joining Community Safety Partners are required to comply with all relevant legislation, including, but not limited to the following:

- Data Protection Act 2018 and General Data Protection Regulation (GDPR) 2017/679, May 2018
- Human Rights Act 1998
- Freedom of Information Act 2000
- Computer Misuse Act 1990
- Regulation of Investigatory Powers Act 2000
- Information Security Policy or equivalent
- Statutory Instrument 1831.

CONNECTION AGREEMENT

THIS AGREEMENT is made on the day of 2018

BETWEEN

(1) **POLICE AND CRIME COMMISSIONER FOR HAMPSHIRE, ISLE OF WIGHT, PORTSMOUTH AND SOUTHAMPTON** of St Georges Chambers, St Georges Street, Winchester, Hampshire, SO23 8AJ ("**Commissioner**") and

(2) **[**[1] **]**
[1. Insert your Organisation's name and address] ("**Joining Community SafetyPartner**")

(collectively "**the Parties**" and independently known as "**the Party**")

WHEREAS

(1) The Commissioner has entered into an agreement ("**the Service Agreement**") with Unilink Limited ("**Supplier**") for the provision of a SafetyNet+ System ("**SafetyNet+**") to the Commissioner and other partners ("**Community Safety Partners**").

(2) The Service Agreement includes provision for the Community Safety Partners to access SafetyNet+.

(3) This Agreement governs the arrangements and commitments between the Parties in relation to a Community Safety Partner accessing SafetyNet+ from 12th November 2018 ("the Commencement Date").

IT IS HEREBY AGREED between the Parties as follows:

1. Except where otherwise stated, references to clauses and schedules are to clauses of and schedules of this Agreement.

2. Following the entering into of this Agreement by the Joining Community Safety Partner, the Joining Community Safety Partner shall be responsible for and hereby accepts sole and exclusive liability for all costs (including reasonable legal costs), losses, damages, claims, demands, expenses and/or liabilities, whether direct or indirect, incurred as a consequence of that Joining Community Safety Partner's breach of this Agreement and /or its failure to comply with its obligations under this Agreement and agrees to indemnify the Commissioner (and (where applicable) any other Community Safety Partner) against any liability that may arise as a consequence thereof.

3. The Joining Community Safety Partner will provide the Commissioner with all necessary co-operation in order to ensure access to and use of the SafetyNet+.

4. The Joining Community Safety Partner acknowledges and agrees that the Agreement provides access to and use of the SafetyNet+ and does not grant any title to it.

5. Notwithstanding the provisions within clause 8.10 of this Agreement, the Joining Community Safety Partner authorizes the Commissioner to engage with the Supplier under the Service Agreement.

4. CODE OF CONNECTION

4.1 The Joining Community Safety Partner will be bound by the Code of Connection ("CoCo") attached at Schedule 1.

4.2 In signing this Agreement, the Joining Community Safety Partner confirms that it has read and understood the CoCo document attached.

4.2 The Joining Community Safety Partner also confirms that it will complete and return the Annual Declaration of SafetyNet+ Code of Connection Compliance (at Schedule 2) within 28 days of the anniversary of the Commencement Date each year.

5. SECURITY OPERATING PROCEDURES FOR USERS

5.1 The Joining Community Safety Partner will be bound by the Security Operating Procedures for Users ("SyOPs") attached at Schedule 5.

5.2 In signing this Agreement, the Joining Community Safety Partner confirms that:

5.2.1 it has read and understood the SyOPs document attached at Schedule 5;

5.2.2 all personnel within the Joining Community Safety Partner's organisation who will have access to SafetyNet+ ("Authorised Users") have read and signed a copy of the SyOPs document and that the Joining Community Safety Partner has retained a copy of these documents; and

5.2.3 all Authorised Users will adhere to the security standards against which SafetyNet+ must be operated to assist in the safe and efficient exchange of information within SafetyNet+.

6. REPORTING OF INCIDENTS

6.1 The Joining Community Safety Partner will inform the Commissioner immediately when it becomes aware of a potential attack, an actual or suspected breach of security or any significant change to the organisation that may affect the security of SafetyNet+. The Joining Community Safety Partner acknowledges that failure to do so may result in revocation of its access to SafetyNet+.

7. CONFIDENTIALITY

7.1 The following definitions apply in this Agreement.

Confidential Information: all confidential information (however recorded or preserved) disclosed by a party or its employees, officers, representatives or advisers (together its **Representatives**) to the other party and that party's Representatives in connection with this Agreement concerning:

7.1.1 the terms of this Agreement;

7.1.2 any information that would be regarded as confidential by a reasonable business person relating to:

a) the business, affairs, clients, service providers, plans, intentions, or market opportunities of the disclosing party; and

b) the operations, processes, product information, know-how, designs, trade secrets or software of the disclosing party (or of any member of the group of companies to which the disclosing party belongs); and

c) log-in details and passwords for accessing SafetyNet+; and

7.1.3 any information developed by the parties in the course of carrying out this Agreement.

7.2 The term "**Confidential Information**" does not include any information that:

7.2.1 is or becomes generally available to the public (other than as a result of its disclosure by the receiving party or its Representatives in breach of this clause); or

7.2.2 was available to the receiving party on a non-confidential basis prior to disclosure by the disclosing party; or

7.2.3 was, is or becomes available to the receiving party on a non-confidential basis from a person who, to the receiving party's knowledge, is not bound by a confidentiality agreement with the disclosing party or otherwise prohibited from disclosing the information to the receiving party; or

7.2.4 was known to the receiving party before the information was disclosed to it by the disclosing party; or

7.2.5 the parties agree in writing is not confidential or may be disclosed; or

7.2.6 is developed by or for the receiving party independently of the information disclosed by the disclosing party.

7.3 Each party shall keep the other party's Confidential Information confidential and shall not:

7.3.1 use such Confidential Information except for the purpose of exercising or performing its rights and obligations under this Agreement ("**Permitted Purpose**"); or

7.3.2 disclose such Confidential Information in whole or in part to any third party, except as expressly permitted by this clause 7.

7.4 With the exception of the Confidential Information set out in clause 7.1.2c) above, a party may disclose the other party's Confidential Information to those of its Representatives who need to know such Confidential Information for the Permitted Purpose, provided that:

7.4.1 it informs such Representatives of the confidential nature of the Confidential Information prior to disclosure; and

7.4.2 at all times, it is responsible for such Representatives' compliance with the confidentiality obligations set out in this clause 7.

7.5 The Confidential Information set out in clause 7.1. above must be kept confidential by the user at all times and the user is not permitted to share this Confidential Information except with other authorised users or as required under clause 7.6 below.

7.6 A party may disclose Confidential Information to the extent required by law, by any governmental or other regulatory authority or by a court or other authority of competent jurisdiction or in accordance with the Commissioner's obligations under the Data Protection Legislation, provided that, to the extent it is legally permitted to do so, it gives the other party as much notice of such disclosure as possible.

7.7 The provisions of this clause 7 shall survive for a period of six years from termination of this Agreement.

8. DATA PROTECTION

Data Protection Legislation: (i) the GDPR, the LED and any applicable national implementing Laws as amended from time to time

(ii) the DPA 2018 to the extent that it relates to processing of personal data and privacy;

(iii) all applicable Law about the processing of personal data and privacy;

Data Protection Impact Assessment: an assessment by the Controller of the impact of the envisaged processing on the protection of Personal Data.

Controller , **Processor**, **Data Subject, Personal Data, Special Category Data; Personal Data Breach** , **Data Protection Officer**: take the meaning given in the GDPR.

Data Loss Event: any event that results, or may result, in unauthorised access to Personal Data held within SafetyNet+ under this Agreement, and/or actual or potential loss and/or destruction of Personal Data in breach of this Agreement, including any Personal Data Breach.

Data Subject Access Request: a request made by, or on behalf of, a Data Subject in accordance with rights granted pursuant to the Data Protection Legislation to access their Personal Data.

DPA 2018: Data Protection Act 2018

GDPR: the General Data Protection Regulation *(Regulation (EU) 2016/679)*

LED: Law Enforcement Directive *(Directive (EU) 2016/680)*

Protective Measures: appropriate technical and organisational measures which may include: pseudonymising and encrypting Personal Data, ensuring confidentiality, integrity, availability and resilience of systems and services, ensuring that availability of and access to Personal Data can be restored in a timely manner after an incident, and

regularly assessing and evaluating the effectiveness of the such measures adopted by it.

Sub-processor: any third Party appointed to process Personal Data on behalf of the Commissioner related to this Agreement.

8.1 The Parties acknowledge that for the purposes of the Data Protection Legislation, the Joining Community Safety Partner is the Controller, the Commissioner is the Processor and the Supplier is the Sub-Processor. The only processing that the Commissioner is authorised to do is listed in Schedule 4 by the Joining Community Safety Partner and may not be determined by the Commissioner.

8.2 The Commissioner shall notify the Joining Community Safety Partner immediately if it considers that any of the Joining Community Safety Partner's instructions infringe the Data Protection Legislation.

8.3 The Commissioner shall provide all reasonable assistance to the Joining Community Safety Partner in the preparation of any Data Protection Impact Assessment prior to commencing any processing.

8.4 The Commissioner shall, in relation to any Personal Data processed in connection with its obligations under this Agreement:

(a) process that Personal Data only in accordance with Schedule 4, processing may not be determined by the Commissioner unless it is required to do so by law. If it is so required the Commissioner shall promptly notify the Joining Community Safety Partner before processing the Personal Data unless such notification is prohibited by Law;

(b) ensure that it has in place Protective Measures, which have been reviewed and approved by the Joining Community Safety Partner as appropriate to protect against a Data Loss Event having taken account of the:

(i) nature of the data to be protected;

(ii) harm that might result from a Data Loss Event;

(iii) state of technological development; and

(iv) cost of implementing any measures;

(c) ensure that:

i) the Commissioner personnel do not process Personal Data except in accordance with this Agreement (and in particular Schedule 4);

ii) it takes all reasonable steps to ensure the reliability and integrity of any Commissioner personnel who have access to the Personal Data and ensure that they:

(A) are aware of and comply with the Commissioner's duties under this clause;

(B) are subject to appropriate confidentiality undertakings with the Commissioner or any Sub-processor;

(C) are informed of the confidential nature of the Personal Data and do not publish, disclose or divulge any of the Personal Data to any third Party unless directed in writing to do so by the Joining Community Safety Partner or as otherwise permitted by this Agreement; and

(D) have undergone adequate training in the use, care, protection and handling of Personal Data; and

(d) not transfer or process Personal Data outside of the EEA/EU (as applicable)

(e) at the written direction of the Joining Community Safety Partner, delete or return Personal Data (and any copies of it) to the Joining Community Safety Partner on termination of the Agreement unless the Commissioner is required by Law to retain the Personal Data.

8.5 Subject to clause 8.6, the Commissioner shall notify the Joining Community Safety Partner immediately if it:

(a) receives a Data Subject Access Request (or purported Data Subject Access Request);

(b) receives a request to rectify, block or erase any Personal Data;

(c) receives any other request, complaint or communication relating to either Party's obligations under the Data Protection Legislation;

(d) receives any communication from the Information Commissioner or any other regulatory authority in connection with Personal Data processed under this Agreement;

(e) receives a request from any third Party for disclosure of Personal Data where compliance with such request is required or purported to be required by Law; or

(f) becomes aware of a Data Loss Event.

8.6 Taking into account the nature of the processing, the Commissioner shall provide the Joining Community Safety Partner with full assistance in relation to either Party's obligations under Data Protection Legislation and any complaint, communication or request made under clause 8.5 (and insofar as possible within the timescales reasonably required by the Joining Community Safety Partner).

8.7 The Commissioner shall maintain complete and accurate records and information to demonstrate its compliance with this clause. This requirement does not apply where the Commissioner employs fewer than 250 staff, unless:

(a) the Joining Community Safety Partner determines that the processing is not occasional;

(b) the Joining Community Safety Partner determines the processing includes special categories of data as referred to in Article 9(1) of the GDPR or Personal Data relating to criminal convictions and offences referred to in Article 10 of the GDPR; and

(c) the Joining Community Safety Partner determines that the processing is likely to result in a risk to the rights and freedoms of Data Subjects.

8.8 The Commissioner shall allow for audits of its Data Processing activity by the Joining Community Safety Partner or the Joining Community Safety Partner's designated auditor.

8.9 The Commissioner shall designate a data protection officer if required by the Data Protection Legislation.

8.10 Before allowing any Sub-processor to process any Personal Data related to this Agreement, the Commissioner will:

(a) notify the Joining Community Safety Partner in writing of the intended Sub-processor and processing;

(b) obtain the written consent of the Joining Community Safety Partner;

(c) enter into a written agreement with the Sub-processor which give effect to the terms set out in this clause 8 such that they apply to the Sub-processor; and

(d) provide the Joining Community Safety Partner with such information regarding the Sub-processor as the Joining Community Safety Partner may reasonably require.

8.11 The Commissioner shall remain fully liable for all acts or omissions of any Sub-processor.

8.13 The Joining Community Safety Partner and Commissioner may, at any time on not less than 30 Working Days' notice agree to revise this clause by replacing it with any applicable controller to processor standard clauses or similar terms forming part of an applicable certification scheme (which shall apply when incorporated by attachment to this Agreement).

8.14 The Parties agree to take account of any guidance issued by the Information Commissioner's Office and may on not less than 30 Working Days' notice agree to amend this Agreement to ensure that it complies with any guidance issued by the Information Commissioner's Office.

9. FREEDOM OF INFORMATION ACT

Information: has the meaning given under Section 84 of the Freedom of Information Act 2000;

Request for Information: a request for information or an apparent request under the Code of Practice on Access to Government Information, Freedom of Information Act or the Environmental Information Regulations;

9.1 Both parties acknowledge that the other party is subject to the requirements of the FOIA and the EIR and shall assist and co-operate each other (at their own expense) to enable the other party to comply with these information disclosure requirements.

9.2 Each party shall:

9.2.1 provide the other party with a copy of all Information in its possession or power in the form that the other party requires within five Working Days (or such other period as the party may specify) of the party requesting that Information; and

9.2.3 provide all necessary assistance as reasonably requested by other party to enable the other party to respond to a Request for Information within the time for compliance set out in section 10 of the FOIA or regulation 5 of the EIR.

9.3 Each party shall be responsible for determining at its absolute discretion whether the Information is commercially sensitive and if it:

9.3.1 is exempt from disclosure in accordance with the provisions of the FOIA or the EIR; or

9.3.2 is to be disclosed in response to a Request for Information, and in no event shall that party respond directly to a request for information unless expressly authorised to do so by the other party.

9.4 Each party acknowledges that the other party may, acting in accordance with the Secretary of State for Constitutional Affairs' Code of Practice on the discharge of public authorities' functions under Part 1 of FOIA (issued under section 45 of the FOIA,), be obliged under the FOIA or the EIR to disclose Information:

9.4.1 without consulting with the other party; or

9.4.2 following consultation with the other party and having taken its views into account

9.5 Each party shall ensure that all Information produced in the course of this Agreement or relating to this Agreement is retained for disclosure and shall permit the other party to inspect such records as requested from time to time.

9.6 Each party acknowledges that any lists or schedules provided by it outlining Confidential Information are of indicative value only and that the other party may nevertheless be obliged to disclose Confidential Information in accordance with clause 8.6.

10. TERMINATION

10.1 The Joining Community Safety Partner may terminate this Agreement by providing one month's notice in writing. Upon serving notice to terminate the Joining Community Safety Partner must also confirm (in writing) that it has closed down any cases that they were the lead Community Safety Partner for. If such confirmation is not received then the notice to terminate will not be valid.

10.2 The Commissioner may terminate this Agreement if the Joining Community Safety Partner does not access for SafetyNet+ for a period of six months or more. The Commissioner will seek confirmation from the Joining Community Safety Partner as to whether they still require access to SafetyNet+. If access is no longer required or no response is received to this request, the Commissioner may terminate this Agreement immediately.

10.3 The Commissioner may terminate this Agreement if the Joining Community Safety Partner commits a material breach of any term of this Agreement which breach is

irremediable or (if such breach is remediable) fails to remedy that breach within a period of 30 days after being notified in writing to do so.

GENERAL

11. The Contracts (Rights of Third Parties) Act 1999 does not apply so as to give to a person who is not a party to this Deed of Accession a right under it.

12. This Agreement shall be governed by and construed in accordance with English Law.

13. This Agreement is personal to the Parties and no Party shall assign, transfer or purport to assign or transfer to any other persons any of its rights or obligations or sub-contract any of its obligations under this Agreement.

14. Any notice required or permitted to be given by a Party to the other Party under this Agreement shall be in writing and addressed to the other Party at its principal office.

15. This Agreement is executed in two counterparts, both of which when taken together shall constitute one and the same instrument.

IN WITNESS whereof the Parties have executed and delivered this agreement as a deed on the day and year first above written:

The Common Seal of
POLICE AND CRIME COMMISSIONER FOR HAMPSHIRE, ISLE OF WIGHT, PORTSMOUTH AND SOUTHAMPTON
was hereunto affixed in the presence of:

(Authorised signatory)

……

[Box 1 - The Commissioner]

The Common Seal of
[2]
[2.Insert your Organisation's name in the field above]

was hereunto affixed in the presence of:

(Authorising signature)

……

[Box 2]

Alternative options for Parties without a Common Seal are available below:

Executed as a deed by
[2]
[2. Insert your Organisation's name in the field above]

acting by [3], a director
and [3], [a director **OR** its secretary]
[3.Insert signatory name]

……
Director Signature

……

Director or Secretary Signature

[Box 3]

Executed as a deed by
[2]
[2.Insert your Organisation's name in the field above)

acting by [3] and
[3], two of its charity trustees.
[3.Insert signatory name]

……
Charity trustee

……
Charity trustee

[Box 4]

Notes for the Joining Community Safety Partner: Please complete box 2, 3 or 4 above as appropriate for your Organisation to execute a Deed; manually adjust the job roles to reflect your Organisation if appropriate and provide a wet signature(s).

SCHEDULE 1

CODE OF CONNECTION

Security Requirements

1. Physical

1.1 You must ensure that buildings and areas which house SafetyNet+ assets or where SafetyNet+ can be accessed from have adequate physical security in order to prevent unauthorised access to the system and / or the information.

1.2 Your organisation should ensure your users comply with any guidance and restrictions contained in your organisation's home working policies, which should, as a baseline, ensure users' homes comply with the 'Secure By Design' standards.

1.3 SafetyNet+ data must only be accessed in an environment appropriate to the data contained within.

2 Vetting

2.1 Those non-police personnel accessing SafetyNet+ must have had the Baseline Personnel Security Standard. This includes the following four checks

- Establishing and confirming claimed identity; and
- Entitlement to work and reside in the UK; and
- Employment history in the last 3 years explored and any gaps discussed; and
- Basic disclosure (unspent criminal record check).

2.2 New organisations interested in signing up to SafetyNet+ need to be sponsored by their local Community Safety Partnership and authorised by the CSP Manager.

2.3 For the Supporting Families Programme, new organisations need to be sponsored by their HCC co-ordinator.

3 Training

3.1 You must ensure that all staff to be granted access to SafetyNet+ within your organisation have both completed the relevant training (training can be cascaded) and signed the Security Operating Procedures (SyOPs) document.

3.2 Your Community Safety Partnership lead for SafetyNet+ will be able to advise you on how to access training.

3.3 Your organisation gives assurance that an Information Assurance culture is embedded across the organisation with local business processes and training in place to enable effective and secure use of information and to react and manage security incidents.

3.4 Staff must be trained to understand that they are responsible for securely handling any information that is entrusted to them in line with local business processes.

4 Classification

4.1 The classification of information stored on SafetyNet+ will be no more than "Official" under the Government Security Classification Program.

4.2 ALL information must be handled with care to prevent loss or inappropriate access, and deter deliberate compromise or opportunist attack.

5 Need to know

5.1 You undertake to ensure that SafetyNet+ Access is given only to those who need it to undertake their work effectively. You accept responsibility for ensuring such use is lawful and meets the purpose of this connection and that you have a lawful basis to process and share the information with relevant organisations in SafetyNet+.

5.2 You undertake to ensure that an appropriate Information Sharing Agreement is in place between you and the organisations with whom you wish to share your information before sharing commences. A template Information Sharing Agreement is attached at Schedule 3 which should be utilised and customised in order to detail the basis of your sharing arrangements.

5.3 You agree to forward a copy of your completed Information Sharing Agreement to the System Administrator to log and record.

6 Confidentiality and Integrity of SafetyNet+

6.1 You agree that your organisation will uphold the Confidentiality, Integrity and Availability and reputation of SafetyNet+.

6.2 You agree to ensure your organisation complies with all relevant legal requirements including those of the Data Protection Act 2018, General Data Protection Regulation 2018, Freedom of Information Act 2000, Computer Misuse Act 1990 and Regulation of Investigatory Powers Act 2000.

6.3 You agree to make all reasonable efforts to inform users of the system that they are subject to auditing and monitoring.

6.4 You agree that your organisation briefs, trains or otherwise formally disseminates information to staff about their secure use of the SafetyNet+ as laid down in this documentation set.

7 Continued access to SafetyNet+

7.1 You agree to ensure that any user in your organisation with access to SafetyNet+, who subsequently ceases to have a lawful purpose to access it, has that access removed in a timely manner.

7.2 You agree to nominate a single point of contact in your organisation to administer your own users, regularly review (at least six-monthly) who has access and ensure that all such personnel agree to the Security Operating Procedures.

7.3 You agree to ensure challenge to any user within your organisation identified as not contributing to SafetyNet+ to ensure they have a continued lawful purpose for access.

7.4 You agree to inform the System Administrator if your organisation no longer has any users who have continued access to SafetyNet+, or if your organisation ceases to have lawful purpose to access SafetyNet+.

7.5 Re-Approval is subject to the submission of a Code of Connection Annual Declaration of Code (Schedule 2).

8 Security Operating Procedures (SyOps)

8.1 You agree to ensure that all SafetyNet+ users in your organisation have signed the SyOPs and that these signed SyOPs are retained for reference.

8.2 You agree to ensure you users abide by the SyOps to assist in the efficient, secure and consistent operation of SafetyNet+ across multiple agencies.

9 Commitment to Review and Audit

9.1 You agree to regularly review and audit your organisation's data entered onto SafetyNet+ to ensure acceptable levels of data quality are met, a consistent approach to data entry and that safeguards are in place to not put each other partner's data at risk.

9.2 The review cycle should consist of:

- A minimum of 60 days for caseworker review,
- A minimum of 90 days for supervisory review.

9.3 You agree to an annual audit by your nominated SafetyNet+ auditor to monitor data quality and compliance with legislation and to ensure cases managed are progressing and reviewed.

9.4 You agree to assist the OPCC in monitoring compliance with the CoCo to ensure SafetyNet+ continues to be a safe and secure partnership information database.

SCHEDULE 2

ANNUAL DECLARATION OF SAFETYNET+ CODE OF CONNECTION COMPLIANCE

(To be completed by your Organisation's Single Point of Contact for SafetyNet+)

1. **Review of Code of Connection:**

1.1 I confirm that I have reviewed the existing SafetyNet+ Code of Connection document

1.2 I declare that the content of the SafetyNet+ CoCo document is still valid;

1.3 Where significant changes have occurred since the last renewal/commencement date, I declare that I informed the SafetyNet+ System Administrator of the changes, on the following date:-…….

1.4 I confirm that I will notify the SafetyNet+ System Administrator of any changes that take place after this declaration.

2. **Review of Users:**

2.1 I declare that all my organisation's current SafetyNet+ users have a legitimate purpose to access the system and access control lists are reviewed on a 6 monthly basis.

3. **Review and Audit:**

3.1 I declare that this organisation has ensured all of its users have read and accepted the SyOPs document. Records of this have been retained to support this statement;

3.2 I declare that this organisation has complied with the review and audit obligations outlined in the code of connection for this 12 month period and records have been retained to support this statement.

Organisation Name: ……..

SafetyNet+ SPOC Name: ……..

SafetyNet+ SPOC's signature: ……..…

SafetyNet+ SPOC's email address: ……

Date: ……..

Please take a copy of this declaration for your records.

Please supply a copy to the SafetyNet+ System Administrator.

SCHEDULE 3

INFORMATION SHARING AGREEMENT
BETWEEN JOINING COMMUNITY SAFETY PARTNERS

Notes for the Joining Community Safety Partner: Please complete yellow highlighted areas with details as appropriate for your Organisation.

1. Introduction

1.1 [1] is committed to tackling Crime and Disorder across Hampshire, Isle of Wight, Portsmouth and Southampton and work, on a regular basis, with members of [2] Community Safety Partnership in order to make Hampshire, Isle of Wight, Portsmouth and Southampton safer and provides a framework for action.
[1.Insert your organisation's name] [2.Insert geographic area]

1.2 SafetyNet+ is a secure partnership database for information sharing, joint risk management and problem solving for multi-agency work across Hampshire, Isle of Wight, Portsmouth and Southampton. SafetyNet+ is administered on behalf of Community Safety Partners by the Office of the Police and Crime Commissioner (OPCC).

2. Objectives and purpose of the Information sharing

2.1 The purpose of this agreement is to facilitate the safe and secure exchange of information between Community Safety Partners to enable action to be taken to support community safety priorities and prevent crime and anti-social behaviour within the local authority area. It will incorporate measures aimed at:

- Facilitating a coordinated approach that targets crime and anti-social behaviour
- Facilitating a coordinated approach to safeguard vulnerable people and victims
- Facilitating the collection and exchange of relevant information.

2.2 The signatory organisations (Joining Community Safety Partners) to this agreement agree that information shared under this arrangement between SafetyNet+ Partners will only be used for the purposes set out in this section of this agreement and will not be used for any other purpose including commercial or marketing purposes.

2.3 This agreement sets out the framework for the sharing of personal data between the parties as data controllers. It defines the principles and procedures that the parties shall adhere to and the responsibilities the parties owe to each other.

2.4 This agreement is in place to inform the reasons and methods of sharing, sharing for other purposes and other information is not covered by this agreement.

2.5 Data can only be used for the purpose shared and cannot be shared to third parties without written permission. Information that may prejudice an ongoing investigation will not be shared unless there is an overriding safety requirement.

2.6 This agreement has been formulated to facilitate the exchange of information between partners. It is, however, incumbent on all partners to recognise that any information shared must be justified on the merits of each case.

3. What data will be shared and how long will it be kept?

3.1 The signatory organisation will share on SafetyNet+ nominal details and activity details as and when appropriate between their own organisation and other relevant case workers only in accordance with Section 2 of this document.

3.2 Personal data will only be used for the specific purpose for which it was obtained.

3.3 The recipient of the information is required to ensure the security of the information shared with them, in accordance with the Code of Connection and Security Operating Procedures. If the recipient of the information extracts information from SafetyNet+ to their own systems they should document the source and retain only as long as necessary in accordance with their organisation's data retention policy.

3.4 All necessary, adequate and up to date records will be retained on SafetyNet+ for a period of seven years from the date of closure of the case channel. The organisation leading on a case channel will ensure this requirement is met and provide authorisation for the deletion of the identified channel and case file if no other active channels remain.

3.5 The signatory organisation will ensure their SafetyNet+ supervisors regularly review their cases in accordance with the Code of Connection and close channels and cases upon the date of the last significant activity in order to comply with clause 3.4.

3.6 The personal data to be shared will consist of information relating to individuals recorded and may include the following data sets :

Names, dates of birth, addresses, details of the commission or alleged commission of offences, details of proceedings relating to offences committed or alleged to have been committed (including sentencing), photographs, identification features and health information.

Location data, details of professional contacts, details of appropriate groups and individuals therein, problem solving activities in partnership and community engagement, KINS and neighbourhood police profiles.

4 Data Controller

4.1 Each signatory organisation will be the data controller as defined in the General Data Protection Regulation (GDPR) and Data Protection Act 2018 (DPA 2018) (and any

successor legislation) for the personal data it holds and will accordingly decide which SafetyNet+ Partners its information will be shared with within SafetyNet+

4.2 Each signatory organisation confirms that it is registered with the Information Commissioner's Office as a Data Controller.

4.3 Each signatory organisation will ensure that any personal data received under this agreement will only be used for the purposes defined in section 2.

4.4 Each signatory organisation as a Data Controller acknowledges its obligations under the GDPR and DPA 2018 when processing personal data, which can include collecting, storing, amending and disclosing data.

4.5 Each signatory organisation agrees that they will only process personal data shared under this agreement within the EU.

5 Arrangements for the safe transmission of data

5.1 The personal data will be shared securely between signatory organisation through the use of SafetyNet+.

5.2 Once the personal data is entered on SafetyNet+ and it will be shared with relevant SafetyNet+ partners only on a need to know basis to ensure that it is protected and is not easily accessible.

5.3 All authorised users must ensure that they take appropriate measures against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to personal data.

5.4 Each signatory organisation will adhere to the specific security requirements set out in the Code of Connection.

5.5 Each authorised user for the signatory organisation will adhere to the operating requirement set out in the Security Operating Procedures.

6. Legal Justification for Sharing the Data

[3].

[3. Insert your Organisation's Legal Justification for Sharing the Data]

7. Fair Processing/Privacy Notices

7.1 The signatory organisations to this agreement recognise their duty under the GDPR to provide information pro-actively and on request to individuals and about how their information is processed.

7.2 Each signatory organisation will ensure that their privacy notices give details of the processing of personal data and will be provided when the data is collected from a data subject.

8. Responsibilities when Sharing Information

General

i. Each signatory organisation shall be responsible for ensuring that they have technical, organisational and security measures in place to protect the personal data and to ensure the lawful use of such information as shared on SafetyNet+ under this Agreement.

ii. Each signatory organisation accepts responsibility for independently or jointly auditing compliance.

iii. Each signatory organisation shall ensure that their authorised users comply with their rules and policies in relation to the protection and use of shared data and that these staff have received sufficient training and are aware of their individual responsibilities in relation to data protection and the confidentiality, integrity and availability of personal data. Each organisation will ensure that appropriate sanctions and disciplinary procedures are in place to deal with non-compliance.

iv. Each signatory organisation shall have a written policy for the retention and disposal of the personal data shared under this Agreement.

Personal Data

v. Personal data may only be shared where there is a specific lawful purpose under Article 6 GDPR and Article 9 GDPR (when the sharing includes Special Category Data) and Article 10 (when the sharing includes Criminal Conviction data).

vi. Each signatory organisation is responsible for ensuring it has a specific lawful basis for sharing any and all Personal Data and Special Category Data before the data is shared within SafetyNet+.

vii. Each signatory organisation shall be aware that consent should only be relied on as the basis for processing and sharing the data where there are no other legal basis under the GDPR. Partners shall be aware that a data subject may withdraw consent without detriment at any time to the processing of their personal data.

viii. If the sharing of personal information covered by this Agreement is based on the informed consent from the data subject or carer, each signatory organisation shall be aware that it must be evidenced by a clear affirmative action. Pre-ticked boxes are not adequate. Data subjects must be informed of their right to withdraw consent. A copy of each party's organisation privacy notice should be made available upon request to the relevant Community Safety Partnership (as referred to in Section 7.2).

ix. Staff of a signatory organisation may only be permitted access to the personal data shared on SafetyNet+ under this Agreement when necessary in order for them to perform their duties in connection with the services they are required to deliver.

x. This Agreement does not permit unrestricted access to the personal information held by the other signatory organisations. It sets out the parameters for the safe and secure sharing of information for a justifiable need to know purpose.

xi. Each signatory organisation shall be responsible for ensuring every member of its staff with access to the personal data shared under this Agreement is aware of and complies with their obligation under the GDPR, DPA 2018, their common law duty of

confidentiality and the responsibility to disclose information only to those who have a right to see it (see section 4 above).

xii. Each signatory organisation shall ensure that any of its staff accessing information follow the principles and standards that have been agreed and incorporated within this Agreement.

9. Restrictions on use of Information Shared

9.1 All information must only be used for the purpose(s) specified in this agreement.

10. Security

10.1 The signatory organisation shall have appropriate technical and organisational measures in place to protect the security, confidentiality, integrity and availability of the personal information (both electronic and hard copy) during all stages of processing. (e.g. transfer, storage, access and deletion).

10.2 Each signatory organisation will adhere to the specific security requirements set out in the Code of Connection.

11. Training

11.1 All signatory organisations will ensure that any authorised users processing information shared under this Agreement are trained in data protection and are fully aware of their responsibilities to maintain the accuracy, security and confidentiality of personal information in an efficient and lawful manner. Authorised users will also be made aware of the requirements to provide privacy notices when sharing or receiving personal data.

11.2 Each signatory organisation must appoint a Single Point of Contact (SPOC) who will receive training and ensure training is cascaded within their organisation. Each Community Safety Partnership will have a trained SPOC who can deliver training locally.

12. Individual Responsibilities

12.1 Every authorised user of the signatory organisation is responsible for the safekeeping of any information they obtain, handle, use and disclose on SafetyNet+.

12.2 Every authorised user should know how to obtain, use and share information they legitimately need to do their job in line with their organisation's policies and procedures.

12.3 All authorised users of Signatory Organisations should follow the guide-lines set out in this Agreement and in the Security Operating Procedures, and seek advice when necessary.

13. Data Accuracy, Rectification, Erasure and Portability

13.1 Each signatory organisation will ensure that the personal data they process and share on SafetyNet+ under this agreement is accurate and up to date.

13.2 Each signatory organisation shall inform the other SafetyNet+ Partners of any rectification or erasure of personal data or restriction of processing as required under Article 19 GDPR.

14. Subject Access Requests

14.1 Each signatory organisation will process Subject Access Requests for the information it holds in line with their existing policies and practices, redirecting requestors under existing procedures, when the request is for data not held or owned by that organisation.

14.2 For the avoidance of doubt personal information supplied by other signatory organisations will be treated as third party.

15. Data Protection Incidents

15.1 Any breaches of security, confidentiality or other violations of shared data must be reported to the sharing organisation as soon as possible and in any case within 24 hours and reported to the SafetyNet+ System Administrator.

15.2 Any breach of information by a signatory organisation is their responsibility. Each signatory organisation is accountable for any misuse of information supplied and the consequences of such misuse. Each signatory organisation will ensure that appropriate sanctions and disciplinary procedures are in place to deal with disclosures of information by employees in bad faith, or for motives of personal gain.

15.3 The signatory organisations shall provide reasonable assistance as is necessary to each other to facilitate the handling of any data security breach and informing the ICO when required. In the event of a dispute or claim concerning the processing of Shared Personal Data against either or both parties, the parties will inform each other about any such disputes or claims, and will cooperate with a view to settling them amicably in a timely fashion.

15.4 The signatory organisations will ensure that they implement any changes to processes or procedures required as a result of a data incident.

16. Commencement of this Agreement

16.1 Access to SafetyNet will be granted to enable information to be shared with other signatory organisations (Community Safety Partners) from the date when a named individual of each organisation signs the Declaration of Acceptance and Participation (below).

17. Review Arrangements

17.1 This ISA will be reviewed annually.

17.2 Any of the signatories can request an extraordinary review at any time where a joint discussion or decision is necessary to address developments or issues.

18. Termination

18.1 Each signatory organisation to this agreement may withdraw on giving one month's written notice to the other Signatories and the System Administrator.

18.2 Each signatory organisation can bring this Agreement to an end with immediate effect on discovery of any breach of this Agreement.

19. Agreement to abide by this Data Sharing Agreement

We the undersigned agree that the Partner Organisation that we represent will adopt and adhere to this Data Sharing Agreement:

Please sign the 'Declaration of Acceptance and Participation' form below and return to: SafetyNet+ Administrator at: opcc.performance.information@hampshire.pnn.police.uk

DECLARATION OF ACCEPTANCE AND PARTICIPATION
All sections of this form must be completed.

Your Organisation name:	
Your name :	
Your Position:	
Signature:	(Please manually sign)
Date:	
Name(s) and email address(es) of individual(s) acting as Single Point of Contact(s):	
Name(s) of additional individual(s) who will process received data:	*The Single Point of Contact will be contacted for a list of staff personnel who require access.*

SCHEDULE 4

PROCESSING, PERSONAL DATA AND DATA SUBJECTS

1. The Commissioner shall comply with any further written instructions with respect to processing by the Joining Community Safety Partner.

2. Any such further instructions shall be incorporated into this Schedule.

Description Details

The Commissioner personnel who have access to SafetyNet+ and access to the stored Personal data will fulfill the System Administrator role for the purpose of account management and only process that Personnel Data upon instruction by the Joining Community Safety Partner for the purpose of the provision of a user support and user assistance in ensuring the integrity of the Personal Data.

The service provided is to facilitate access to SafetyNet+ to Joining Community Safety Partners across Hampshire, Isle of Wight, Portsmouth and Southampton and administer the system on behalf of Joining Community Safety Partners to include organisation and user account set up, system configuration, maintenance of User Guides and this Agreement, provision of User Support and assistance, liaison with the Supplier on technical faults and system development.

Duration of the processing

The data will only be processed for the duration of the contract unless required longer:

1) for retention purposes; or

2) as required by law and in either of those cases as confirmed in writing by the Data Controller.

Nature and purposes of the processing

Such processing as is necessary to enable the Commissioner to comply with its obligations under this Agreement to include any operation such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of data (whether or not by automated means) etc.

The purpose of the processing is the performance of the Commissioner's obligations under this agreement including the performance of functions required or requested by the customer.

Type of Personal Data Personal / Special Category Data:
[Examples here include:
name,
address,
date of birth,
telephone number,
email address,
images,

health information,
personal data relating to criminal convictions and offences detail, etc].

Categories of Data Subject:
[*Examples here include:*
Staff (including volunteers, agents, and temporary workers),
customers/ clients,
members of the public,
carers or representatives,
children under the age of 18, including students and pupils,
complainants, enquirers or their representatives,
licence and permit holders,
professional advisers and consultants,
service users and their representatives ,
persons contracted to provide a service
traders and others subject to inspection ,
representatives of other organisations]

Plan for return and destruction of the data once the processing is complete UNLESS requirement under union or member state law to preserve that type of data

Unless otherwise agreed in writing all personal data is to be destroyed/ returned at the end of the contract and confirmation of this is to be provided in writing to the Data Controller.

SCHEDULE 5

SECURITY OPERATING PROCEDURES FOR ALL USERS

1 Introduction

SafetyNet+ is a secure partnership database, supplied by UniLink Limited, for information sharing, joint risk management and problem solving for multi-agency work across Hampshire, Isle of Wight, Portsmouth and Southampton. It has been designed to enable Community Safety Partners, supported by the legitimate legal basis for sharing personal and sensitive data, to work together to protect and safeguard those at most risk and jointly manage those that prevent a threat. It facilitates our joint efforts to reduce crime, promote public safety, and create vibrant and inclusive communities.

Sharing data within SafetyNet+ takes place using two main modules; Integrated Case Management (ICM) and Neighbourhood Management System (NMS). Users enter information onto the system via their browser, which is encrypted in transit between the end user's device and the remote application to the server:

- When submitted to ICM, basic nominal identifiers are visible to all ICM users with further layered restrictions to those with access to the relevant, shared casefiles and activities.
- When submitted to Neighbourhood Management system (NMS) this is then visible by all other users assigned to that neighbourhood area. Specific Police data fields are extracted and published to Police.uk.

SafetyNet+ is managed by the Office of the Police and Crime Commissioner on behalf of community safety partner organisations. This SyOPs is produced by the OPCC to establish the operational requirements for SafetyNet+ across multiple agencies. The OPCC provides user assistance and user guides to aid the efficient and consistent operation of SafetyNet+.

New organisations interested in signing up to SafetyNet+ need to be sponsored by their local Community Safety Partnership and authorised by the CSP Manager. For the Supporting Families Programme, new organisations need to be sponsored by their HCC co-ordinator.

A registration form and sign up pack is available from the Police and Crime Commissioner's website via email to: opcc.performance.information@hampshire.pnn.police.uk

2 Routine Operation Requirements

2.1 When you log in to SafetyNet+, you will check the box on the log on screen to state you have read and understand the SyOPs and agree to comply with the instructions therein.

2.2 You are required to have read the SyOPs and confirmed by wet signature prior to being allowed access to the system.

2.3 You should review and sign the SyOPs on an annual basis and confirm to your SafetyNet+ single point of contact that you have a lawful purpose to continue to access the system.

2.4 The SyOPs is a list of requirements you agree to meet to prevent data from SafetyNet+ being lost, misused or abused and to ensure the consistent operation by a large user-base.

2.5 You must comply with these SyOPs and all organisational Information Security (Infosec) strategies, policies and procedures. If you identify a conflict between local procedures and these SyOPs you should contact your SafetyNet+ single point of contact.

3 Security Responsibilities

3.1 When you log in to SafetyNet+, you will check the box on the log on screen to state you have read and understand the SyOPs and agree to comply with the instructions therein.

3.2 It is the responsibility of all authorised users of SafetyNet+ to ensure that the system be used in a secure manner.

3.3 The system and the data it contains are for official use only. All authorised users must treat the system and the information held in a way appropriate to its security classification.

3.4 For further information or clarification contact your Local Supervisor.

4 Allocation of a SafetyNet+ Account

4.1 A formal application for an account should be made to your organisation's SafetyNet+ Single Point of Contact (SPoC), stating your requirement to use the system and the role you will perform.

4.2 When your account has been created, you will receive a set of Identification and Authentication (Id & A) credentials in order to access SafetyNet+.

4.3 You must inform your Local SPoC of any change to your status (e.g. change of role, leaving the organisation etc).

5 Password Management

5.1 You should note that your SafetyNet+ user account and password are exclusively for your use and you must not share your access credentials or access privileges with anyone else.

5.2 Whilst logged on, your access credentials are used to generate an audit trail for every action you perform for which YOU will be held accountable.

5.3 You may keep a written record of your password provided that:

- The record is kept in a sealed envelope marked 'OFFICIAL SENSITIVE – PRIVATE' with your signature over the flap to ensure that any attempt to access the record will be evident; and
- The envelope is kept within a security container suitable for storage of sensitive personal data.
- You must not keep any other written record of your passwords.

5.4 SafetyNet+ is configured to alert you at regular intervals that you will need to change your password.

5.5 You must change your password on first login, or after a system generated password reset. SafetyNet+ will dictate the type and strength of your own required password and will prevent you from entering:

- valid dictionary words or names
- your user account name or organisation name
- a telephone number

- the previous three passwords you have used on the system.

5.6 You should avoid using characters identifiably associated with yourself (e.g. your date of birth, address, nicknames, etc).

5.7 Your account will be temporarily locked if you enter your password incorrectly 3 times in succession. If this occurs, or if you have forgotten your password, you are able to request a reset through the system.

6 Logging on and off

6.1 To access the SafetyNet+ system you will first need to:
- Log into your user profile from the nominated SafetyNet+ machine – that is a device approved for running the SafetyNet+ portal and the IP address registered for authorised access
- Connect to the SafetyNet+ portal through your web browser shortcut
- Enter you SafetyNet+ user name and password.

6.2 Upon completion of a session, you must:
- Log off the SafetyNet+ portal using the sign-out link
- Log off the client device (laptop/terminal)
- You must log off both SafetyNet+ AND your local user profile before allowing anyone else to use your workstation.

7 Use of your SafetyNet Account

7.1 Your account is for your exclusive use only and you must not allow anybody else to use it.

7.2 You must not misuse the SafetyNet+ system. Examples of misuse include, but are not limited to
- any violation of the SyOPs
- any activity that is illegal under national or international law
- making libelous statements relating to individuals or companies
- disclosure of information to individuals who are not authorised to receive it
- introduction of malicious or unauthorised programs on the system
- allowing your account to be used by others
- carrying out network monitoring activities
- use for personal reasons not related to your work
- use for vetting individuals for employment purposes or for reasons not related to the purpose of the system

8 Import of Data

8.1 You must ensure personal data entered onto ICM meets the purposes for sharing as contained in the SafetyNet+ Information Sharing Agreement and only for a legitimate business purpose in accordance with the Data Protection Act 2018 and General Data Protection Regulation (GDPR) 2018.

8.2 The purpose of NMS is to manage location data. Professional contact details relating to neighbourhoods are stored in NMS and such data is deemed personal data.

8.3 Whether in ICM or NMS, the import of data must be made with consideration to whether the audience is appropriate. You must ensure no inappropriate disclosures are made.

8.4 You must not attempt to import data using USB ports, CD/DVD drives, floppy drives or similar whilst in the SafetyNet+ application without the means to scan the input device with a suitable virus/malware/content checker.

8.5 You should be aware of the risk of unintentionally loading malicious software (computer viruses, Trojan horses, etc.) onto your system.

8.6 If you suspect that there may be malicious software in the SafetyNet+ application or your workstation, you must stop using the workstation immediately and report it to your Local Supervisor and SPOC.

9 Export / exchange / Print of data

9.1 Users must only export / exchange information for legitimate business purposes in accordance with the Data Protection Act 2018 and General Data Protection Regulation (GDPR) 2018 and any other legislative, regulatory, organisational or ethical expectations and requirements.

9.2 The local storage of data extracted from SafetyNet+ is not permitted except where it is transferred for a lawful purpose to an approved auditable system within your organisation.

9.3 When data is extraction by organisation that organisation becomes the data controller for that data.

9.4 Any printed material must be handled with the same sensitivity and not contradict these rules. It must be handled in a way which makes accidental or deliberate misuse through disclosure, loss or theft unlikely to occur and easy to detect if it happens.

9.5 In the event that you or other users print data, you must ensure that all print requests are completed. Dependent on your organisation's policy, printed output will if possible bear the Protective Marking "Official".

10 Physical security

10.1 SafetyNet+ information and assets require protection from unauthorised personnel and those without the need to know and use.

10.2 If you leave your terminal you must consider the risks of the system or its information being compromised in your absence and take appropriate measures to minimise this risk.

10.3 To ensure that continued confidentiality, integrity and availability of the SafetyNet application and information assets –

10.4 You Must:

- Ensure that equipment used to access SafetyNet+ is housed in secure areas (CoCo s1.1)
- Ensure the client device (the SafetyNet+ Laptop or desktop) is secured at all times, including locking away laptops, and suitably encrypted if used away from normal office premises
- Ensure visitors into areas storing, processing, manipulating or outputting SafetyNet+ information are escorted at all times unless they are authorised as unescorted visitors
- Challenge anyone not wearing visible identification or anyone you do not recognise
- Comply with a clear desk and clear screen policy

- Log off the SafetyNet+ application when you intend leaving your desk (even momentarily) and lock your computer/account.
- If you intend on being away from your desk or leaving our office unoccupied for an extended period (more than 15 minutes) you should log off completely
- Always position your SafetyNet+ terminal to prevent being overlooked
- If you require assistance from your IT Helpdesk you must close the Safety Net+ application prior to any remote support
- Ensure any portable devices used to log on to SafetyNet+ comply with the above.

10.5 You Must Not;

- Move any item of SafetyNet+ equipment or attempt to make changes to the configuration of SafetyNet+ equipment without explicit permission
- Remove or distribute SafetyNet+ information or equipment without explicit authority
- Make unauthorised documentary records of SafetyNet+ information
- Provide the codes to physical access barriers protecting SafetyNet information to any persons
- Use unauthorised removable media e.g. USB sticks, CD/DVDs, mobile phone data storage
- Use any unapproved IT assets to log on to the SafetyNet+ portal

11 Protective marking

11.1 The protective marking of information stored on SafetyNet+ will be no more than "Official" under the Government Secure Classification (GSC) Program.

12 Incident Management

12.1 You are required to notify your Local SafetyNet+ SPOC immediately if you know or suspect your SafetyNet+ application password is compromised and provide details as to how or why the compromise occurred. This enables immediate revocation of your access privileges and the resetting of your account.

13 Supervisory Roles and Responsibilities

- Local Supervisor
- Local Single Point of Contact (SPOC)
- Local Auditor
- System Administrator (OPCC nominated staff).

13.1 Local Supervisor

You have been nominated as a SafetyNet+ Supervisor responsible for the day-to-day supervision and review of SafetyNet+ cases in your organisation.

You must comply with these SyOPs and all organisational Information Security (Infosec) strategies, policies and procedures. If you identify a conflict between local procedures and these SyOPs you should contact your line manager or Local SPOC.

You must comply with these SyOPs to ensure the lawful, efficient and consistent operation of SafetyNet+ in this multi-agency information sharing platform.

Responsibilities:

- You must ensure compliance with the SyOPs by the system users you supervise within your organisation. All users are required to comply with these SyOPs to ensure the lawful, efficient and consistent operation of SafetyNet+ in this multi-agency information sharing platform.
- Non-compliance with the SyOPs may result in termination of your organisation's access to SafetyNet+ as per the Connection to SafetyNet+ Agreement.
- Where you are notified of change of details of system users, you should notify your Local SPOC.
- You will ensure that data processed on SafetyNet+ will be subject to a review cycle to ensure that active cases are managed within appropriate time limits and that acceptable levels of Data Quality are met.To ensure a consistent approach and manage expectations between multiple partners the review period will consist of a minimum of:

Caseworker review	Every 60 days
Supervisor/manager review	Every 90 days.

13.2 Local Single Point of Contact

You are nominated as a Local SafetyNet+ SPoC for your organisation. You are responsible for the coordination of SafetyNet+ within your organisation and effective operation of the system in your organisation.

You must comply with these SyOPs and all organisational Information Security (Infosec) strategies, policies and procedures. If you identify a conflict between local procedures and these SyOPs you should contact your line manager and the SafetyNet+ System Administrator.

You must comply with these SyOPs to ensure the lawful, efficient and consistent operation of SafetyNet+ in this multi-agency information sharing platform.

Responsibilities:

Account Management

- You must ensure that your organisation has provided a signed up to date SafetyNet+ Connection Agreement and Code of Connection Annual Declaration to the System Administrator
- You must maintain an up to date 'access control list' of individuals authorised to have access SafetyNet+ in your organisation, including their permissions within the application to carry out their duties effectively. The Access Control List must be reviewed on a 6 monthly basis and written record maintained of the review.
- You are responsible for SafetyNet+ user account authorisation within your organisation.
- You must authorise new accounts or changes to existing accounts for users in your organisation that meet all the following criteria:
  - A business requirement to access the SafetyNet+ system
  - Have appropriate security clearance (vetting). See CoCo 5.2.
  - Have received appropriate training
  - Have read SafetyNet+ User Guide
  - Have read and agreed to the SyOPs
  - A signed SyOPs is provided to you and retained.
- When individuals are no longer authorised or no longer have a business need in their role to have access to SafetyNet+ you must ensure that their account is disabled/archived and advise the SafetyNet+ System Administrator.
- You will ensure that all authorised users of the SafetyNet+ application understand their security responsibilities as defined in the SafetyNet+ user SyOPs.

Incident Management

- You must ensure that all actual and suspected security incidents are reported to the SafetyNet+ System Administrator immediately and follow your organisation's incident reporting processes.
- You must immediately report any instance of theft, loss, temporary loss or suspected compromise of protectively marked information or asset giving access to protectively marked information (including keys / PINS / Smartcards) to the System Administrator.
- You must also note and report any actual or potential security vulnerabilities or actual or potential threats to the System Administrator.
- If a password is compromised this must be immediately changed and reported to the System Administrator.
- You must ensure investigation of local security incidents and progression of technical faults by liaising with the relevant departments as necessary.
- In emergency contact UniLink Ltd at 0845 6580 803.

13.3 Local Auditor

You are nominated as a Local SafetyNet+ Auditor for your organisation. You are responsible for ensuring the integrity of data inputted by your organisation.

You must comply with these SyOPs and all organisational Information Security (Infosec) strategies, policies and procedures. If you identify a conflict between local procedures and these SyOPs you should contact your Organisation's SPoC and SafetyNet+ System Administrator.

You must comply with these SyOPs to ensure the lawful, efficient and consistent operation of SafetyNet+ in this multi-agency information sharing platform.

Responsibilities:

Management of Data Quality

- You are responsible for auditing SafetyNet+ to ensure data quality and compliance with the relevant standards for your organisation's inputted data. It is recommended this is undertaken with dip sampling by the auditor role.
- You are also responsible for ensuring your organisation maintains a case review regime and data quality regime which complies with the Code of Connection, in order to ensure that information populated onto and managed on SafetyNet+ by your organisation is of suitable quality to comply with the General Data Protection Regulations Principles and the purpose for which it is processed.

13.4 System Administrator

You have been nominated as a SafetyNet+ System Administrator for the Office of Police & Crime Commissioner in order to manage the system on behalf of all community safety partner organisations accessing SafetyNet+. You are responsible for the administration of the system and assistance to users in the correct and secure operation of the SafetyNet+ application.

The only data processing you are authorised to do is upon the instruction from the data controller and as listed in the Connection Agreement Schedule 4.

You must comply with these SyOPs and all organisational Information Security (Infosec) strategies, policies and procedures. If you identify a conflict between local procedures and these SyOPs you should contact your Senior Manager.

You must comply with these SyOPs to ensure the lawful, efficient and consistent operation of SafetyNet+ in this multi-agency information sharing platform.

Responsibilities:

- Providing User Assistance & Guidance
- Organisation account set up with approval from the CSP Manager
- Access management in accordance with approval from the local SPOC
- Maintaining and reviewing the SafetyNet+ Connection Agreement and Schedules.
- Managing the receipt and storage of signed documentation to support organisation's connection to SafetyNet+
- Publishing an organisation list on the OPCC website with a link to each signed ISA (Schedule 3)
- Investigating and progressing technical faults liaising with UniLink Ltd or relevant departments as necessary
- Recording data loss and security incidents liaising with relevant departments as necessary
- The management of configuration and development changes to SafetyNet+ in consultation with User Groups.

14 Undertaking to abide by the SyOPs - ALL USERS

In addition to the undertakings that the user must accept each time they log in to SafetyNet+, each user must sign this document to confirm they have read and understood their obligations when using the system.

A copy of this document will be retained by the SafetyNet+ SPOC for your organisation or department.

I, the undersigned, have read and understood the SafetyNet+ SyOPs document, version 1 and agree to abide by it

Name (print name): …….....

Organisation: ……

SafetyNet+ Role (please tick all that apply):

- ☐ **Authorised User** (Roles with general use and update)
- ☐ **Local Supervisor** (Roles with supervision of other users' cases)
- ☐ **Local Single Point of Contact**
- ☐ **Local Auditor**
- ☐ **System Administrator** (OPCC nominated staff only)

Signature: …….....

Date: ……...

Please take a copy of this declaration for your records.

Please supply a signed copy to the SafetyNet+ SPOC for your organisation or department.