POLICY

Information Sharing

Policy owners	Head of Information Management
Policy holder	Information Compliance Manager
Author	Information Sharing Officer

Approved by

Legal Services	N/A
Policy owner	May 2017
JJNCC	07/06/2017

Note: *By signing the above you are authorising the policy for publication and are accepting responsibility for the policy on behalf of the Chief Constables.*

Publication date	15/06/2017
Review date	15/06/2021
APP Checked	March 2017
Code of Ethics Checked:	June 2017

Note: *Please send the original Policy with both signatures on it to the Norfolk CPU for the audit trail.*

Index

Legal Basis

Legislation specific to the subject of this policy document

Section	***Act (title and year)***
	Statutory Code of Practice for the Management of Police Information issued under The Police Act 1996
S. 115	Crime and Disorder Act 1998
Sch 2.1.2	Data Protection Act 2018

Other legislation which you must check this document against (required by law)

Act (title and year)
Human Rights Act 1998 (in particular A.14 – Prohibition of discrimination)
Equality Act 2010
Crime and Disorder Act 1998
Health and Safety at Work etc. Act 1974 and associated Regulations
General Data Protection Regulation and Data Protection Act 2018
Freedom Of Information Act 2000
Civil Contingencies Act 2004

Other Related Documents

- Code of Practice on the Management of Police Information
- Guidance on the Management of Police Information (MoPI).
- NPCC Community Security Policy
- Authorised Professional Practice
- College of Policing Code of Ethics
- Norfolk and Suffolk Constabularies' Standards of Professional Behaviour

1. Introduction

1.1 Information is a corporate resource for the police service. As such, there is a requirement for common processes to manage information appropriately. Police information is defined in the Guidance on the Management of Police Information (MOPI), as information that is required for a policing purpose. In order to operate effectively, police forces need to be able to share such information within the service, with partner agencies/organisations, and with the general public.

1.2 Partnership working requires the two way flow of information to facilitate good relations with other agencies/organisations, reduce crime and disorder, and help make communities safer. However, there must be robust processes in place to ensure information sharing is legal and appropriate which are subject to ongoing critique and review.

2. Principles of Sharing

2.1 Policing requires information to be shared within the Police Service, with partner agencies/organisations and with the general public. Opportunities should be actively sought to share non-personal information to facilitate the flow of information and improve positive relations with partner agencies/organisations.

Personal information; which is defined in the Data Protection Act 2018 as data which relates to a living individual who can be identified:

- from those data, or
- from those data and other information which is in the possession of, or likely to come into the possession of, the controller, and includes any expressions of opinion about the individual and any indication of the intentions of the Controller or any other person in respect of the individual;

should be shared where appropriate, subject to certain safeguards. It is therefore important to establish a legal gateway and/or a policing purpose as the basis for sharing police information.

2.2 There are two types of information sharing – 'one off sharing' and 'systematic sharing' as detailed below.

<u>One off Sharing</u>

2.3 One off information sharing relates to instances where the Constabularies decide, or are asked to share information in situations which are not covered by an Information Sharing Agreement. In some cases this may involve a decision about sharing being made in conditions of real urgency, for example in an emergency situation.

- Example: An Officer attends a RTC and one of those involved is known to the Police for violence against individuals in authority or uniform. The individual is taken to hospital via ambulance and following a risk assessment and taking into account the decision making criteria below, the Officer is of the opinion that staff in the ambulance and hospital may be at risk of harm from the individual. A proportionate and timely disclosure would be appropriate.

Systematic Sharing

2.4 Systematic information sharing relates to the routine sharing of information between organisations for an agreed purpose. Systematic sharing is underpinned by the use of Information Sharing Agreements between the Constabularies and partner agencies/organisations. The Information Sharing Agreement will clearly detail the specific requirements and processes, including the legal basis for sharing information on a formalised basis.

- Example: The Multi Agency Safeguarding Hub is an environment within which information sharing with other partner members is essential to ensure risks to individuals are managed. Information is shared on a daily basis to identify and mitigate the risks. A signed Information Sharing Agreement is in place to record the purpose, legal basis and information sharing processes. An Information Sharing Agreement does not mean that all information is shared with any organisation or in all circumstances. Each decision is considered on a case by case basis and information is shared where it is appropriate and safe to do so or justified on the basis of appropriate safeguarding.

2.5 Use of standardised Information Sharing Agreements ensures consistency in the way information is shared. It allows the Constabularies to place conditions on the way information is handled by another agency. It ensures information is shared lawfully, and helps to build confidence in the role the police play in protecting the public and their personal information.

2.6 An Information Sharing Agreement must be used whenever police seek or are requested to share information frequently with other agencies. The Constabularies' Information Sharing Agreement is designed for use when other agencies wish to access information held by the Constabularies.

2.7 However, similar formal documentation should also be used whenever police wish to frequently or regularly access information held by another agency. Whilst the documentation referred to is designed for the Constabularies' use, it may also be used as a template for other agencies/organisations wishing to formalise processes for the Constabularies to access their information.

2.8 An exception to the above requirements is where there is already a national protocol in place (such as between NPCC and UK Border

Agency) that fulfils or exceeds the requirements of our own information sharing agreements.

2.9 Systematic information sharing should be proactive as well as reactive. It is therefore expected that Officers and staff will identify and facilitate systematic information sharing wherever there is an anticipated need rather than wait for partner agencies/organisations to approach the constabularies with a request to share information.

3. Information Sharing Processes

3.1 With all information sharing where the disclosure will relate to personal data then it must be done in line with the General Data Protection Regulation (GDPR) and Data Protection Act (DPA) 2018, in particular the data protection principles and Article 6, 9 and 10 of the GDPR and Schedule 1, parts 1, 2 and 3 of the DPA 2018, the Human Rights Act 1998 and the common law duty of confidence as well as references in other relevant legislation.

3.2 All disclosure decisions must be made on a case by case basis. Whether administering a frequent arrangement or a one-off request, the disclosure decision-making process is the same, i.e. they have to satisfy the requirements of the law.

3.3 All personnel have the authority to share information on a case by case basis after taking into account the criteria and guidance below. However, should advice be required after considering the criteria and guidance, please use the following contacts:

- Suffolk – Data Protection Decision Maker, Ext 3514 or email dataprotection@suffolk.pnn.police.uk
- Norfolk – Data Protection Decision Maker, Ext 2801 or email dataprotection@norfolk.pnn.police.uk
- Guidance is also available within the 'Disclosure of Information Guidance' which can be located on the Information Management pages of the intranet.

3.4 It will not always be possible or practical to refer all requests for advice on the disclosure of personal data to the Specialist Advisors, particularly where cases are deemed an emergency.

<u>One off Sharing</u>

3.5 There are occasions when publicity in the local media is a method to be used to locate an individual. Prior to the media release, authorisation is required from an Inspector rank or higher. Examples of media releases and the rank of the Officer required to authorise the request are below. Following authorisation, contact the Corporate Communications Department to arrange the release.

- An Inspector or above has to approve:

▪ High risk missing person. For further information refer to the Missing and Absent Persons Policy and Honour Based Abuse, Forced Marriage and Female Genital Mutilation Policy.

  - Public appeals to identify potential suspects of offenders through CCTV images.

- A Chief Inspector or above has to approve:
  - Public appeals to locate a wanted person.

3.6 A Schedule 2.1.2 Form is used to access personal data held by an external organisation and is required to progress a criminal investigation. The Form is completed by the officer in charge of the investigation or an individual involved in the investigation and has to be approved by an Officer of Inspector rank or higher prior to submission to the organisation. Completing and submitting the form to an external organisation can require a disclosure. The form needs to provide sufficient information for the organisation receiving the form to make an informed decision on whether to disclose the information. Relevant and necessary information to assist the organisation to make an informed decision is required to be disclosed on the form.

3.7 The decision to disclose/share personal data requires careful judgement to ensure data protection and human rights conditions are balanced and evidenced as necessary, to achieve compliance with the policing purpose.

3.8 The following guidance is provided to help determine whether the personal data being considered for disclosure/sharing is necessary. Non-personal data is not subject to the considerations. For all disclosure/sharing of personal data the following considerations should be followed and documented:

- Establish whether satisfied with the requester's identity and there is no doubt that they are who they say they are;
- Establish whether the requester has a sufficient 'need to know' and have made it clear exactly what information is being sought and provided sufficient detail to locate the information;[1]*
- Identify exactly what purpose the disclosure will serve and what may be compromised if the disclosure is not made;*
- Identify from the above Legal landscape which category the disclosure/sharing may fall into;*

[1] *There may already be an Information Sharing Agreement in place covering this type of request – check the Information Sharing Agreement Central Register on the 'W' Drive under Information Management/Information Compliance/Data Protection/Org/Reports and Publications

- Establish whether a Policing purpose can be satisfied, which is supported by the Information Asset Owner and line manager of Inspector rank or higher;

  Note: If the disclosure is extremely urgent i.e. to preserve life or prevent a death and that delay would hinder this, do not delay in making a disclosure – release immediately and record the decision making at a later stage.

- Establish whether the disclosure is absolutely necessary or whether the purpose can be achieved without the need to share personal data.
- Establish whether the information intending to be shared is accurate, reliable and up-to-date.
- Establish whether the information intending to be shared is no more and no less than is necessary and proportionate to achieve the purpose. This will involve balancing persons Human Rights through assessing the privacy intrusion upon the person about whom the information is being disclosed against the duty owed to protect the other parties/public through the intended sharing process and establishing whether such disclosure is proportionate. This requires a risk-assessed decision making process to be followed often identifying the risk of harm to all parties, which in some cases can be complex and may require specialist/legal advice.
- Establish whether the information intending to be shared was acquired under an obligation of confidence and if so, ensure the disclosure can be satisfied by one of the following conditions. This may require an assessment of the impact of the disclosure upon a person's privacy against any harm/risks associated with other persons, such as the vulnerable, if the disclosure does not take place:
  - There is a legal requirement to disclose,
  - There is an overriding duty to the public, and
  - The individual about whom the data relates has consented to the disclosure.
- Establish if there is a need to remove specific information that could identify innocent/third parties that are not connected with the matter.
- Establish if disclosing excessive information that could compromise an informant's/whistleblower's identity could cause harm/damage which needs to be removed from the disclosure.
- Establish if the information being disclosed/shared requires any additional security measures to be applied by the receiving party, over and above that which may already be contained in any Information Sharing Agreement. It is advisable to discuss any security measures with the Information Security Unit at the onset in the event additional costs/measures may be identified. If the disclosure is a one-off, the following security statement should accompany the information intending to be disclosed, as a minimum:

"In receiving this information, you must ensure that it is protected to a minimum standard commensurate with the Protective Marking of OFFICIAL or legacy protective marking of RESTRICTED (depending on age of information), unless otherwise marked. As such, you undertake to ensure that the information will be used only for the purpose for which it was requested, only provide the information to those with an appropriate level of 'need to know', will exercise strict security controls so as to prevent any unauthorised access/disclosure and securely destroy it when no longer required. Strict security control includes, but is not limited to:

- *Secure storage of the information when not in use;*
- *Securely transporting the information within sealed envelopes and by using recorded, trackable delivery mechanism; and*
- *Limiting any coping/reproduction of the information.*

For further information on security control, please refer to your Information Security Manager."

- Establish how long the receiving party is expected to retain the information and ensure the receiving party is made aware of this.*
- Establish whether the receiving party needs to make contact before making any further disclosures of the information to the individual about whom the data relates (under Article 15 of the GDPR or Section 45 of the Data Protection Act – Subject Access). Considerations should be given as to the nature of the information and whether disclosure to the individual themselves would compromise a police operation.

Systematic Sharing

3.9 Whenever a request is received from another agency/organisation, or a need for systematic sharing is identified, the Information Sharing Agreements Central Record should be checked to see if an Information Sharing Agreement, with the relevant organisation and for the same purpose, already exists. All current Constabularies' Information Sharing Agreements and known National Agreements can be found on the W drive at:

W:\Collaboration\Information Management\Information Compliance\Data Protection\Org\Reports and Publications\ISA Central Record

3.10 If an Information Sharing Agreement exists that appears to fully meet the requirements of the new request, contact either the Designated Officer for the Constabularies listed on the agreement who will advise whether the existing agreement is identical and adequate. If any uncertainty exists, contact the Information Sharing Officer for advice on the below details:

- E-mail: dataprotection@suffolk.pnn.police.uk

- Telephone: Ext 2058 (03 2058 from Norfolk) (external 01473 782058)
- Address: Data Protection Team, Information Compliance Unit, Suffolk PHQ

3.11 If it is adequate no further action beyond advising the partner agency/organisation is necessary.

3.12 When making a decision to share or not under the terms of the Information Sharing Agreement, an officer or staff member must record the decision and rationale, including:

- What information was shared and the purpose;
- Who it was shared with;
- Date it was shared;
- Rationale and legal basis for sharing (i.e. the Information Sharing Agreement used);
- Whether the information was shared with or without consent.

It is good practice to record this information on the main record for managing the incident. For example, on the Athena record, in a CAD or the CATS record. If no electronic record exists a PNB entry needs to be made.

3.13 If there is no existing Information Sharing Agreement or the existing agreement does not fulfil the requirements, it will be necessary to draft a new Information Sharing Agreement. The Information sharing questionnaire will need to be completed and sent to the Information Sharing Officer.

3.14 The Information Sharing Officer will perform a risk assessment to ensure the proposed information sharing is legal, necessary and proportionate. This will include an assessment of the security arrangements of the recipient agency/organisation, their approach towards data protection (including confidentiality and third party procedures), their data protection breach procedures, how the information will be stored, how the information will be shared and the risks associated with refusal to grant permission for information sharing.

3.15 With regards to security all Chief Constables are committed to compliance with the NPCC Community Security Policy, and they and Partner Organisations are expected to ensure that all data and information is handled in line with the Her Majesty's Government (HMG) Security Policy Framework, specifically meeting the Mandatory Requirement:

"Departments and Agencies must have an information security policy setting out how they and any delivery partners and suppliers will protect any information assets they hold, store or process to prevent

unauthorised access, use, disclosure, modification, disposal, or impairment, whether intentional or unintentional, through appropriate technical and organisational security measures."

3.16 See Appendix A for the Constabularies' Information Security Policy Statement, which details the security requirements the constabularies expect the receiving agency/organisation to have in place to ensure the constabularies' information is kept secure once shared with them, and is appended to all Information Sharing Agreements. For queries or advice regarding security please contact the Information Security Manager on the below e-mail address:

InformationSecurity@suffolk.pnn.police.uk

3.17 There may be occasions in a multi-agency information sharing initiative that bulk information sharing is required. For example when analysis of past behaviour is required to influence future intervention and support programmes for victims and offenders. The sharing and analysis of information may be considered as an intrusion of individual's privacy. In these cases it is recommended that a Data Protection Impact Assessment (DPIA) is considered. Please refer to the DPIA Policy for further information such as when a DPIA should be conducted and who should conduct the DPIA.

3.18 From an information sharing perspective, a DPIA can identify potential risks in the business processes early on in the project and thereby reduce costs associated with rectifying the issue at a later stage where the necessary changes are problematic to implement. A DPIA will also reassure individuals who are subject to the sharing of personal data, that the Constabularies are following best practice.

3.19 The Norfolk and Suffolk Compliance Officer can assist in the completion of a DPIA and can be contacted via:

- E-mail: compliance@suffolk.pnn.police.uk
- Telephone: Ext 3682 (03 3682 from Norfolk) (external 01473 613682)
- Address: Compliance Team, Information Compliance Unit, Suffolk PHQ

3.20 Further guidance is also available in the Data Protection Impact Assessment Policy.

3.21 When all of the above matters have been satisfactorily addressed and the Information Sharing Officer agrees that the information sharing is legal and necessary, the Information Sharing Officer will draft the Information Sharing Agreement.

3.22 The process for new Information Sharing Agreements will be followed:

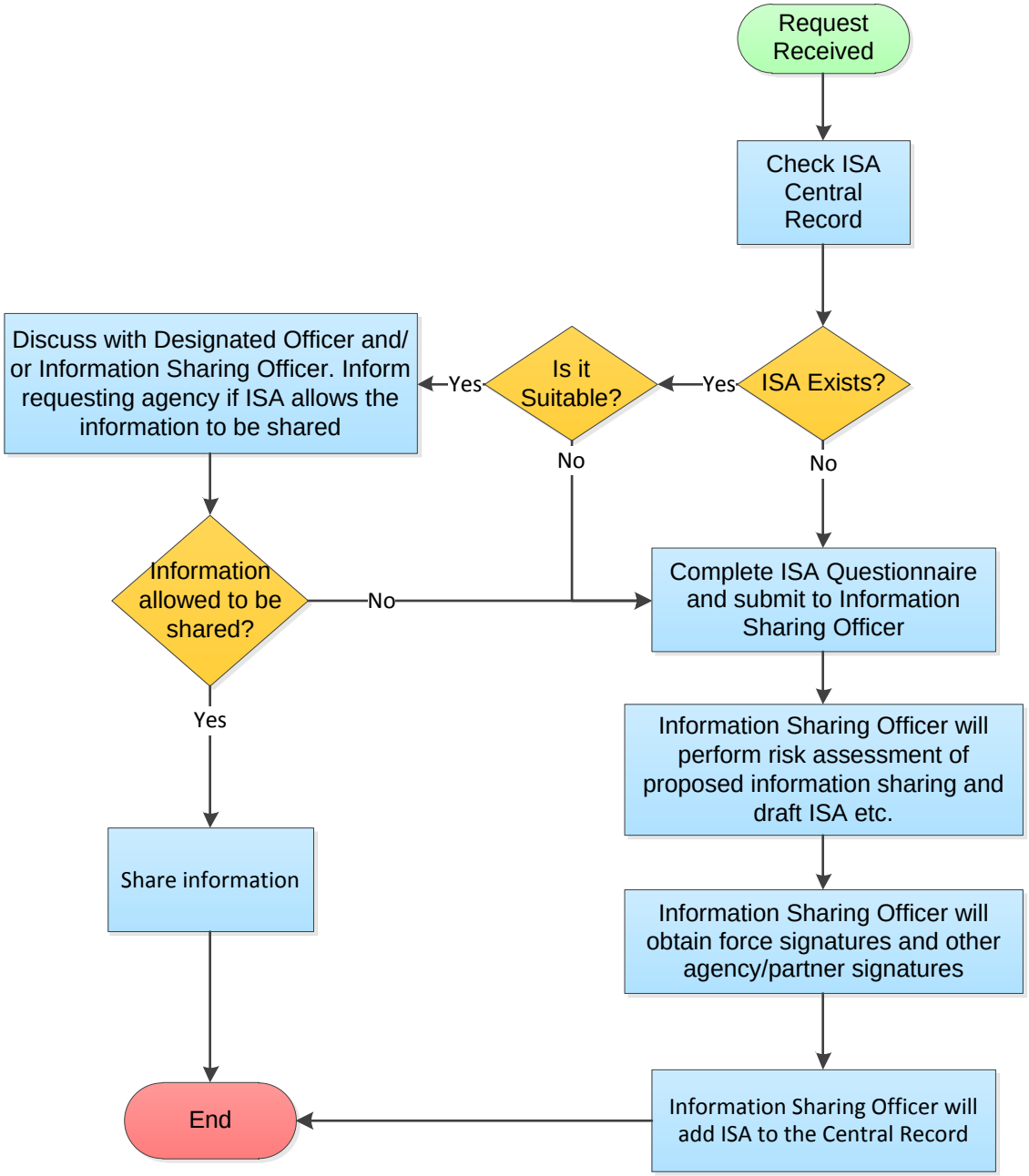
- The Information Sharing Officer will liaise with key stakeholders in the Information Sharing Agreement process until each are satisfied:
    - Information Asset Owner(s).
    - Designated Officer.
    - Information Compliance Manager.
    - Information Security Manager.
    - Information sharing partners.

3.23 When the final version of the Information Sharing Agreement has been agreed by the Head of Information Management and signed off by the Deputy Chief Constables, the Information Sharing Officer will acquire the partnership signatures, inform the relevant business area and record the agreement on the central register.

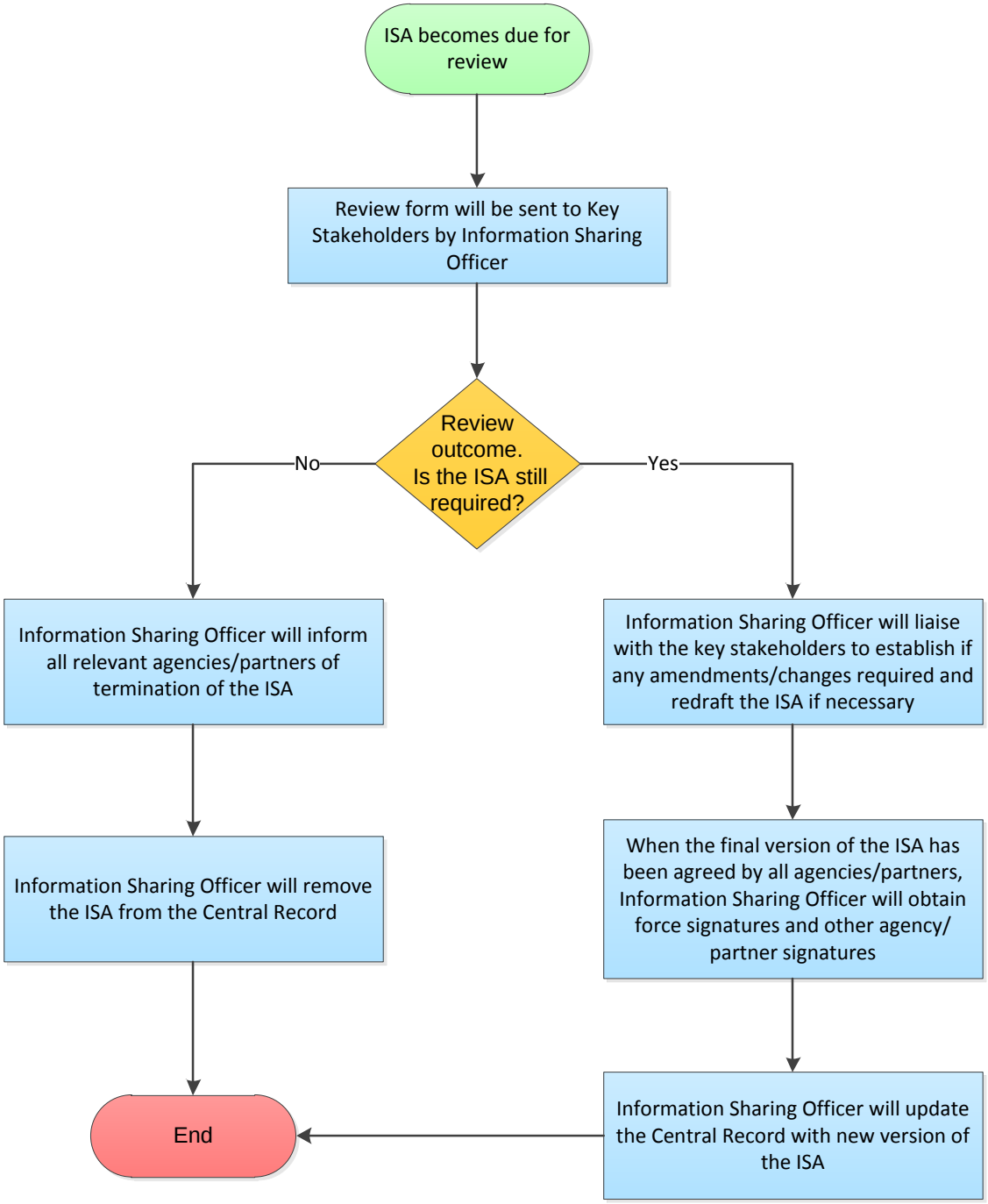
3.24 The Information Sharing Officer will initiate a review of the Information Sharing Agreement on an annual basis, and will liaise with the key stakeholders to establish if the Information Sharing Agreement is still required and if it is, any changes to the information being shared, the processes, the Designated Officers etc.

3.25 The process to review existing Information Sharing Agreements will be followed in the same order as for new Information Sharing Agreement. (As per paragraphs 3.22 – 3.24)

4. Information Sharing Agreement Flowchart



5. Review of Information Sharing Agreement Flowchart



Appendix A – Norfolk and Suffolk Constabularies' Information Security Policy Statement

All Chief Constables are committed to compliance with the Community Security Policy, and they and Partner Organisations are expected to ensure that all data and information is handled in line with the HMG Security Policy Framework, specifically meeting the following Mandatory Requirement:

> 'Departments and Agencies must have an information security policy setting out how they and any delivery partners and suppliers will protect any information assets they hold, store or process (including electronic and paper formats and online services) to prevent unauthorised access, disclosure or loss. The policies and procedures must be regularly reviewed to ensure currency.'

1. Scope

1.1 These Information Security Requirements and Objectives apply to the following:

Roles & Responsibilities

> All persons or parties conducting work for either Signatory regardless of any form of employment, including contractors providing services, agency workers and trainees on vocational or work experience.

Data & Information

a) Whether stored, copied, duplicated or transmitted, all 'soft' (electronic, digital and virtual) data, information and communications on servers, networks, connectivity, ICT kit such as PCs, workstations, laptops, and authorised multimedia devices including USBs, mobile phones, tapes and CDs.

b) Also 'hard' information printed or written on paper or other medium such as whiteboards and flipcharts, and transmitted by any method whatsoever, such as fax or scanner.

c) Additional safeguards should be considered, specified and documented according to the sensitivity and classification of the data, information, and/or circumstances of the Agreement, for example observing operational security, such as precautions against eavesdropping.

Data: The Data Protection Act & Information Commissioner's Office

a) Where Signatories process personal data defined by the Act, they agree to apply security measures, commensurate with the principles of the General Data Protection Regulation 2016/679 and the Data Protection Act 2018, and in particular by applying that personal data shall be: "processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or

unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality')".

b) These Information Security Requirements and Objectives should evidence this principle.

2. Information Security Requirements & Objectives

2.1 To that end, Signatories to this agreement should ensure, document and be able to evidence, that they have in place common technical and organisational security arrangements, evidencing the following appropriate, proportionate and reasonable Information Security Requirements and Objectives:

a) Information Security risk assessments to establish, evaluate and accept risks, and put in place appropriate controls to manage them.

b) Information Security Policies, Guidelines, Processes, Controls and Practices in place to protect, and ensure the confidentiality, integrity and availability of data and information and systems under their control.

c) An Information Security Review process at planned intervals so that, should significant changes occur, this will ensure their continued suitability, adequacy, and effectiveness; i.e. for technological, legal, contractual and regulatory requirements and organisational changes.

2.2 Specifically, they should address the Information Security Requirements and Objectives below.

Information Security Policy

A documented Information Security Policy: should provide governance, management direction and support for information security according to relevant business and organisational requirements, contractual obligations, laws, statutes, regulations and best practices.

Organisation of Information Security

Internal Organisation & External Parties: To manage information security within the organisations, and maintain the security of information and information processing facilities that are accessed, processed, communicated to, or managed by external parties.

Asset Management

Responsibility for Assets & Information Classification: To achieve and maintain appropriate protection of organisational assets, and ensure information receives an appropriate level of protection.

Human Resources Security

Prior to, During & After Employment. Training & Awareness: To ensure that employees, contractors, third parties, and other users understand their responsibilities, and are suitable for the roles they are considered; reducing the risk of theft, fraud or misuse of facilities; and are aware of information security threats and concerns, their responsibilities and liabilities, and are equipped to support security policy in their normal work, reducing the risk of error; and to ensure that all users exit or change employment in an orderly manner. Information security programmes should be available and imparted to all relevant users.

As an organisation Suffolk and Norfolk Constabularies have given an undertaking as part of their PSN(P) accreditation that all Police Staff and others who have access to Police data will be vetted in line with ACPO vetting policy, which defines non-police staff as requiring vetting to a minimum of NPPV2.

Physical & Environmental Security

Secure areas & Equipment Security: To prevent unauthorised physical access, damage and interference to the organisations' premises and information; and prevent loss, damage, theft or compromise of assets and interruption to the organisations' activities.

Communications & Operations Management

- **Operational Procedures, Responsibilities & Third Party Service Delivery Management:** To ensure the correct and secure operation of information processing facilities; and implement and maintain the appropriate level of information security and service delivery in line with third party service delivery agreements;
- **System Planning, Acceptance & Protection Against Malicious & Mobile Code:** To minimise the risk of systems failures; and protect the integrity of software and information;
- **Back-up & Network Security Management:** To maintain the integrity and availability of information and information processing facilities, and ensure the protection of information in networks and the protection of the supporting infrastructure.
- **Media Handling, Exchange of Information & Monitoring:** To prevent unauthorised disclosure, modification, removal or destruction of assets, and interruption to business activities; maintain the security of information and software exchange internally and with any external entity; and detect unauthorised information processing activities.
- **Electronic Commerce Services:** To ensure their security, and secure use.

Access Control

- **Business Requirement for Access Control & User Access Management:** To control access to information, ensuring authorised user access, preventing unauthorised access to information systems.
- **User Responsibilities & Network Access Control:** To prevent unauthorised access, compromise, theft of information and information processing facilities; and access to networked services.
- It is imperative that user accounts are unique to enable the tracking of specific activity to named individuals.
- User activity must be correlated to a user via the use of a unique identifier. Each user connected to the network shall be assigned a unique user ID in order that it can be used for authentication of that individual user.
- The access control will be covered by the Information Security policies and therefore will be sufficient to manage the risk to the organisation.
- **Operating System, Access, Application, & Information Access Control:** To prevent unauthorised access to operating systems; and information held in application systems.
- **Mobile Computing & Teleworking:** To ensure information security when using mobile computing and teleworking facilities.

Information Systems Acquisition, Development & Maintenance

- **Security Requirements of Information Systems & Correct Processing in Applications:** To ensure that security is an integral part of information systems, and prevent errors, loss, unauthorised modification or misuse of information in applications.
- **Cryptographic Controls & Security of System Files:** To protect the confidentiality, authenticity or integrity of information by cryptographic means, and ensure the security of system files.
- **Security in Development, Support Processes & Technical Vulnerability Management:** To maintain the security of application system software and information, and reduce risks resulting from exploitation of published technical vulnerabilities.

Information Security Incident & Breach Management

To report information security threats, events and weaknesses ensuring those associated with information systems are communicated to allow timely corrective action; and manage incidents and improvements, ensuring a consistent and effective approach is applied to information security incidents.

Business Continuity Management

To counteract interruptions to business activities and to protect critical business processes from the effects of major failures of information systems or disasters and to ensure their timely resumption.

Compliance with Legal Requirements

To avoid breaches of any law, statutory, regulatory or contractual obligations, and of any security requirements, and that they are met wherever applicable; and to ensure compliance of systems with organisational security policies and standards, and to maximise the effectiveness of and to minimise interference to/from the information systems audit process.