Information Sharing

Standard Operating Procedure

Notice:

This document has been made available through the Police Service of Scotland Freedom of Information Publication Scheme. It should not be utilised as guidance or instruction by any police officer or employee as it may have been redacted due to legal exemptions

Owning Department	Professionalism and Assurance
Version Number	3.00 (Publication Scheme)
Date Published	23/09/2019

Compliance Record

Equality and Human Rights Impact Assessment (EqHRIA) Date Completed / Reviewed:	28/03/2018
Information Management Compliant:	Yes
Health and Safety Compliant:	Yes
Publication Scheme Compliant:	Yes

Version Control Table

Version	History of Amendments	Approval Date
1.00	Initial Approved Version	21/10/2013
2.00	Completely revised to support changes in the Data Protection Act 2018, including the General Data Protection Requirement (GDPR) and Law Enforcement Directive (LED).	25/05/2018
3.00	Minor change to hyperlink within Appendix ‘A’	23/09/2019

Contents

Appendices

1. Purpose

1.1 This Standard Operating Procedure (SOP) supports the Police Service of Scotland, hereafter referred to as Police Scotland, Policy (or policies) for:

- Data Protection
- Information Security
- Records Management

1.2 This SOP sets out the framework for the sharing of personal information between Police Scotland and external organisations, either within or outwith the bounds of an Information Sharing Agreement (ISA).

1.3 This SOP provides guidance on the process for developing and approving an ISA.

1.4 The SOP is aimed at Police Officers and Members of Police Staff who may require to share information as part of their role.

2. Definition and Types of Information Sharing

2.1 For the purposes of this SOP, information sharing (also referred to as data sharing) is defined as 'The disclosure of personal information from one or more organisations to a third party organisation or organisations.'

2.1.1 The rules outlined in this SOP apply to requests for information received by Police Scotland and information requests made by Police Scotland.

2.2 Information sharing is a type of processing as defined within Data Protection legislation. Data Protection legislation has been reformed and will now consist of the General Data Protection Regulation (GDPR), which has direct effect in the UK as of 25 May 2018, and the Data Protection Act 2018 (DPA 2018).

2.2.1 Within the United Kingdom, DPA 2018 transposes the European Union Data Protection Directive 2016/680 (known as the EU Law Enforcement Directive 2016, or 'LED') into domestic legislation. Part 3 of the DPA 2018 specifically applies to processing for law enforcement purposes, i.e. the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.

2.2.2 This SOP is written to ensure compliance with the reformed legislation.

2.3 Information sharing provides benefits to data subjects (i.e. the individuals about whom information is shared), Police Scotland and partner organisations. It can also bring wider societal benefits. However, the rights of the data subjects concerned should be at the core of any decisions about whether to share the information. The benefits to be gained by that data subject should be balanced with their rights, including their right to privacy.

2.4 Information is a key resource to Police Scotland and it should be shared in compliance with applicable law to ensure the confidentiality, availability and integrity of that information. Appropriate sharing will minimise the risk of data breaches and potential enforcement action by the Information Commissioner's Office (ICO) or other regulators, increase public trust and protection for the public, reduce reputational risk from inappropriate sharing and reduce the risk of complaints and disputes regarding the sharing of information.

2.5 There are two main types of information sharing:

- Routine, pre-planned sharing;
- One-off decisions in situations of operational urgency.

2.6 Examples of routine, pre-planned sharing are:

- A reciprocal exchange of information (e.g. sharing between police and Registered Social Landlords in relation to Anti-Social Behaviour);
- Pooling information and making it available to each other (e.g. Multi-Agency case conferences);

  or

- Several organisations pooling info and making it available to third parties (e.g. following roll-out of a referral scheme, police and partners pooling the data gathered and providing it to a third party to evaluate the scheme).

2.7 Situations of operational urgency requiring one-off decisions may include:

- Requesting information from a power company regarding a property to progress a drugs investigation;
- Sharing information about an individual with a specialist reporting agency to prevent a crime;
- Sharing information with another organisation about an individual at risk of serious harm.

2.8 Where information sharing is pre-planned and routine, the proposed process should be checked against the Data Protection Principles. Any identified risks should be weighed against the benefits of the sharing, and rules and procedures established to minimise identified risks. If the sharing is likely to result in a high risk to the rights and freedoms of individuals, or involves the use of new technology, a Data Protection Impact Assessment (DPIA) may be required. (See Section 7.6, below).

2.9 The rules and procedures are usually outlined in an Information Sharing Agreement (ISA), which sets out the formal framework for the transfer of personal data (see Section 7, below). This should ensure that:

- Information is shared lawfully;
- The risk of data breaches occurring is minimised;

- The type of information to be shared is defined and the procedures to share it have been assessed as lawful, relevant and proportionate.

2.10 However, a proactive decision may be made to share one-off information or a request for information might be received where there is no ISA in place. It may still be lawful and possible to share the information, but Police Scotland should be able to demonstrate the rationale behind the decision and the steps that have been taken to ensure compliance with data protection legislation.

2.11 Information shared with the Crown Office and Procurator Fiscal Service (COPFS) and the Scottish Children's Reporter Administration (SCRA) is classed as routine. However, as there is a requirement under legislation to provide information to these organisations, an ISA would not be required. However, due to the complexity of some of the processes involved in provision of information to COPFS and SCRA, ISAs may be put in place outlining specific procedures to be followed.

3. Information Sharing Rules

3.1 General Rules

3.1.1 All information sharing, whether it is routine or one-off, should follow the rules below:

- **Why** is the information to be shared? (Identify the policing purpose and the 'Legal Gateway' which permits the sharing. (See Sections 3.2. and 3.3, below);
- **Who** is it going to be shared with? (provide details of the partners in the data sharing relationship);
- **What** information can be shared? (detail the specific types of information, e.g. names, addresses, previous convictions);
- **When** is the information going to be shared? (e.g. in response to a partner's request or a particular event, or on our own initiative as a result of an investigation);
- **How** is the information going to be shared? (Email, hand delivery, verbally at meetings – security and access to and storage of information should be addressed).

3.1.2 Every decision to share should be on a case by case basis and should be recorded in an auditable format, including the decision making rationale (see Section 6 below for further guidance on recording information).

3.2 Policing Purposes

3.2.1 There **must** be a legitimate reason, i.e. a 'Policing Purpose', for obtaining and recording the information in the first place. Once a Policing Purpose has been identified, and a potential need for information sharing established, a Legal Gateway **must** be identified which will ensure that the information goes to the correct recipient organisation that is able to take action which supports that original policing purpose.

3.2.2 The Policing Purposes are defined as:

- Protecting life and property;
- Preserving order;
- Prevention and detection of crime;
- Apprehension and prosecution of offenders;
- Any duty or responsibility arising from common or statute law.

3.2.3 The definition of Policing Purpose is broader than 'Law Enforcement Purposes' as defined within the DPA 2018, i.e. processing by the police for:

"The purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security".

3.2.4 A Policing Purpose will also encompass duties relating to reduction or prevention of harm to an individual, where the harm is not occurring as a result of a criminal offence (for example, dealing with a suicidal individual, or with wellbeing concerns).

3.2.5 Therefore, the reason for the information sharing **must** be assessed as to whether it falls under

- GDPR (i.e. where it is not crime related);

  or

- Law Enforcement under Part 3 of the DPA 2018 (criminal offence related)

3.3 Legal Gateway

3.3.1 In addition to the identified policing purpose, an appropriate legal gateway **must** be identified. The term 'Legal Gateway' is used in relation to the mechanism (or legal power) which allows information to be shared. This refers to parts or sections within different pieces of legislation that either expressly require or permit the sharing of information, or which, when interpreted, imply that information may be shared.

3.3.2 Accordingly; where legislation pertaining to an area of police business states that “A constable **must** provide relevant information…” This provides a statutory obligation. If, however, legislation states that “A constable may provide relevant information…” This permits sharing at the constable’s discretion.

3.3.3 Certain Data Protection legislation also provide legal gateways. Examples given in the previous Data Protection Act 1998 (Schedule 3) include ‘for the prevention and detection of crime’, or ‘for the purposes of legal proceedings’.

3.3.4 More than one legal gateway may be utilised during an information sharing process. For example; information about an individual who has offended may initially be shared with Police Scotland using the crime and taxation exemption (formerly more commonly referred to as the ‘s29 exemption’ under the previous Data Protection Act 1998). Services of Third Sector Organisations (TSO - voluntary, community and/or not-for-profit organisations) may subsequently be identified, and signposting to the organisation or information sharing with the individual’s consent may then be the most appropriate route.

3.3.5 If no policing purpose and legal gateway is identified, information **cannot** be shared. It is crucial to document the rationale if a decision not to share is reached, in case the decision is subsequently questioned as part of a review/inquiry.

3.4 Fair Processing/Privacy Notices

3.4.1 Data Protection law requires that processing of a data subject’s information is both lawful and fair – this means that it should be clear to individuals the purposes for which their information is going to be used. Where data relating to children is being processed, information **must** be supplied using plain language, appropriate to their age.

3.4.2 Fair processing is carried out by supplying a Privacy Notice. This is an accessible document which provides individuals with information about how their personal data will be used. The provisions of the DPA 2018 allow for the fact that law enforcement agencies may not be able to be completely transparent about their activities, for example if it would undermine or compromise an investigation. Therefore if the information sharing is for Law Enforcement purposes, it may be sufficient to have a privacy notice available that individuals can be directed to which provides general details of the information sharing (for example on the Police Scotland website), rather than having to proactively inform an individual about the sharing.

3.4.3. However, in some circumstances there is a requirement to actively communicate the information (for example by reading out a script, or sending a letter), as failure to do so would result in unfairness to the individual. The following are circumstances where active communication is required:

- The purpose for sharing falls under GDPR rather than Law Enforcement;

- An individual would not expect the data to be shared or would object to the sharing;
- Sharing/not sharing the information would have a significant effect on the individual;
- The sharing involves organisations an individual might not expect;

  or

- The sharing is being carried out for a number of different purposes.

3.4.4 Fair processing implications should be considered whether the information sharing is carried out as part of an agreement or on a one-off basis.

3.4.5 ISAs should document the extent to, and the means by which fair processing will be carried out, including whether a bespoke privacy notice is required. Further advice can be obtained from Information Assurance (See Appendix 'H').

3.4.6 If the sharing is one-off, consideration should be given to what an individual can be told without prejudicing the purpose, and if there are any restrictions to what the individual has been told, the reasons should be documented. For example, telling a suspect that their information is being processed may be prejudicial to an investigation, as it may allow the opportunity for evidence to be destroyed.

3.4.7 Further guidance on fair processing can be found within the Police Scotland Data Protection SOP.

4. Legal Powers/Gateways

4.1.1 Section 3.3 (above) provided the definition of a Legal Gateway. This section explains how to assess whether a Legal Gateway exists that will permit information sharing.

4.1.2 Personal information is protected from inappropriate processing, including sharing, by the DPA 2018, the Human Rights Act 1998, Article 8, and the common law duty of confidentiality.

4.2 Common Law Duty of Confidentiality

4.2.1 The duty of confidentiality is not written in statute but has been established by court decisions over time. Duty of confidentiality considerations are often considered in statutory provisions relating to information sharing. For example, s139 (3) of the Antisocial Behaviour etc. (Scotland) Act 2004 contains provisions relating to a duty of confidentiality.

4.2.2. Before considering sharing information about a data subject, consideration should be given as to whether the information would be covered by the common law duty of confidentiality.

4.2.3 Decision making factors should include:

- Is there a quality of confidentiality to the information? (i.e. does it hold a degree of sensitivity and significance?, and is not in the public domain);
- Is there a reasonable expectation of privacy? (E.g. individuals may reasonably expect their information to be passed to a court or other justice organisations to support criminal proceedings. However, a victim or a witness may not reasonably expect that their information would be passed on to other organisations such as TSO providers of support services);
- Is the use of the information unauthorised? (E.g. it would not meet a Policing Purpose, or the use goes beyond what an individual would expect when their information was gathered).

4.2.4 If such information was shared, a breach of confidence would occur unless an exemption applies. The exemptions are:

- There is a legal requirement either through statute (for example, s61 of the Children's Hearings (Scotland) Act 2011, where constables **must** provide information to the Principal Report under certain circumstances) or by a court order;
- The data subject has consented to the sharing (refer to section 4.7 for further details);
- There is an overriding public interest in sharing the information (for example, protection of health and morals, public safety, prevention of crime and disorder and national security).

4.2.5 In deciding whether or not there is an overriding public interest justification, consideration **must** be given to the harm that will be accrued through the failure to disclose the information, and the harm that will accrue by breaching an individual's confidentiality. These considerations **must** be balanced in order to make an appropriate decision.

4.2.6 If disclosures which breach the Common Law Duty of Confidentiality are routinely considered as part of a business process, the considerations required should be built into guidance relating to that business process, and any related ISAs. Otherwise, advice should be sought from an Information Assurance Officer (IAO) or the disclosures should be carried out as per the instructions provided in the Public Interest Disclosure SOP.

4.2.7 Disclosures of information covered by the Common Law Duty of Confidentiality **must** be proportionate, the minimum necessary to achieve the aim, and **must** be recorded in writing. The written record of the disclosure **must** detail why it was necessary to disclose the information, and demonstrate that proportionality has been considered.

4.2.8 Where there is no statutory obligation or consent from the subject, the written record **must** identify the nature of the public interest justification, and the decision **must** be signed off at an appropriate level (Superintendent or above). The disclosure **must** also still comply with the principles of the DPA 2018 (for example, the information **must** be accurate).

4.2.9 A generic process flowchart for processing disclosures subject to the Common Law Duty of Confidentiality has been developed and is shown at Appendix 'G' to this SOP. The process describes all the major elements of such disclosures but it should be noted that every such disclosure must be considered on its own merit, on a case by case basis.

4.3 Data Protection Legislation

4.3.1 The majority of the information that Police Scotland will consider sharing with partners will be personal data or sensitive/special category personal data as defined within the DPA 2018. For further information, see the Police Scotland Data Protection SOP.

4.3.2 Apart from very specific circumstances relating to National Security, where personal data is being shared, a lawful basis from GDPR and/or a condition for processing from the DPA 2018 **must** be satisfied. The lawful basis/conditions applied will depend on whether or not the information is being shared for law enforcement purposes or for another purpose under GDPR (for example, child wellbeing), and whether the information being shared is personal data, special category data or criminal offence data.

4.3.3 For the majority of police information, the most commonly engaged condition for processing/lawful basis is likely to be a function conferred on Police Scotland via the Police and Fire Reform (Scotland) Act 2012, legal proceedings or administration of justice, i.e. sharing relating to the policing purposes. Therefore the lawful basis under GDPR might be Article 6(e) public task (which encompasses the non-criminal elements of the policing purposes), or if it is for the law enforcement purposes (i.e. crime related) it will fall under Part 3 of the DPA 2018.

4.3.4 Further guidance on identifying an appropriate condition for processing/lawful basis can be sought from an Information Assurance Officer (See Appendix 'H').

4.3.5 The sharing of personal/sensitive personal data held by the police can only take place where one of the following criteria is met:

- There is a statutory obligation to disclose;
- There is a statutory power to disclose;
- There is an implied power - there is a policing purpose and the sharing complies with all of the relevant DPA 2018 principles;
- An exemption can be applied as per the Schedules of the DPA 2018;

  or

- The data subject has given their consent to the disclosure.

4.4 Statutory Obligation/Statutory Power

4.4.1 As per Section 4.3 (above), statutory obligations or statutory powers to share conferred under an enactment are a form of Legal Gateway.

4.4.2 Some of the functions will confer a statutory obligation on Police Scotland (we **'must'** take a particular action), and some functions conferred will be discretionary (we **'may'** take a particular action).

4.4.3 Examples of statutory obligations include:

- Part V of the Police Act 1997 (Disclosure Certificates);
- s61 of the Children's Hearings (Scotland) Act 2011 (Constable's duty to provide information to the Principal Reporter)

4.4.4 Examples of statutory powers include:

- s139 of the Antisocial Behaviour etc. (Scotland) Act 2004;
- s5 of the Adult Support and Protection (Scotland) Act 2007 (where the 3-point test is met);
- s36 of the Counter-Terrorism and Security Act 2015 (prevent).

4.5 Implied Power

4.5.1 Implied powers are derived from the legislation which governs an organisation's activities, i.e. the Police and Fire Reform (Scotland) Act 2012, in particular s20 – Constables: general duties. In other words, the policing purposes outlined at Section 3.2 (above).

4.5.2 An implied power should only be used to justify one-off disclosures in very rare circumstances, such as where someone is at serious risk of harm. Using an implied power requires the framework of an ISA in order to fully document the policing purpose, whether the policing purpose falls under GDPR or Law Enforcement, why the information sharing is necessary to meet that policing purpose, what the recipient organisation will do with the information (i.e. what is their statutory remit that would cover processing the information), and demonstrate how all of the DPA 2018 principles are being met (for example, how are we meeting our fair processing obligations).

4.6 Exemptions

4.6.1 Where Police Scotland is considering sharing information and none of the other Legal Gateways are applicable, then consideration could be given to whether there is a suitable exemption. Schedule 2 of the DPA 2018 lists exemptions from the GDPR, for example where processing is required by a court order or is necessary for legal proceedings (equivalent provisions to those under s35 of the Data Protection Act 1998).

4.6.2 The provisions of the exemption formerly under s29 of the Data Protection Act 1998 are now built into Part 3 of the DPA 2018, processing for Law Enforcement purposes. This does not mean that all the data sharing by the Police will be exempt, but it allows for restrictions to certain rights where it can be demonstrated that applying the rights would prejudice the law enforcement purpose.

4.6.3 Where Police Scotland is requesting information from an organisation for prevention or detection of crime/apprehension or prosecution of offenders, that organisation could consider using the crime and taxation exemption to provide the police with the information (see Section 8.5, below).

4.7 Consent

4.7.1 Consent is defined in the GDPR as “any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her”.

4.7.2 The GDPR and DPA 2018 bring additional requirements relating to consent – it **must** be unambiguous, affirmative consent (i.e. all consent will be explicit). There are additional requirements around withdrawal of consent (should be as easy to withdraw as it is to provide), and obtaining granular, specific consent for all aspects of the processing (this will be difficult to achieve if there are many organisations involved, with different pieces of information being relevant to each organisation).

4.7.3 As consent **must** be freely given, there **must** be no imbalance in the relationship between the requestor and the individual – this will make it difficult for public authorities in a position of power over an individual (such as the police) to rely on consent. There **must** be no detriment to an individual if they say no. This does not however mean that it cannot be used for sharing which does not fall under our core public task. For example; where a referral is being made to a TSO which provides a support service. However, the benefits in undertaking such processes **must** outweigh the risks of non-compliance with the legislation.

4.7.4 Adequate information **must** be provided to allow the individual to make an informed decision – any implications **must** be outlined including what will happen if they refuse to provide consent. Individuals **must** have a genuine choice to provide or refuse to provide consent (again, no detriment to them if they say no), otherwise it would not be fair to ask for consent in the first place. In addition, the circumstances under which the police are attending may not be conducive to ensuring consent is informed.

4.7.5 There **must** be an auditable, active communication to signify that consent has been provided. It does not have to be in writing, but that is the easiest means of recording and auditing consent, for example by obtaining a signature in a police notebook after an explanation has been provided and consent agreed. A notebook entry should also be made if consent was requested and refused. Alternatively, a bespoke consent form could be designed to support an information sharing process. If there is no auditable record of what was agreed, it will be difficult to justify the sharing if there is a subsequent complaint by an individual.

4.7.6 Consent will only last as long as the processing to which consent was given continues. Individuals have the right to withdraw their consent at any time. Processing of information prior to withdrawal will still be valid, however processing **must** cease once consent is withdrawn. Any partners affected by withdrawal of consent **must** be updated about the change in status.

4.7.7 Consent can also be varied or refused – consideration of what would happen under those circumstances may help identify another, more appropriate, condition for processing.

4.7.8 Consent only legitimises the disclosure of that individual's information – it cannot be used to justify sharing someone else's information (another condition for processing would have to be sought for sharing that information).

4.7.9 There are particular difficulties where children are concerned:

- The child **must** have the capacity to understand the nature and consequences of information sharing relating to them. If the child does not have capacity, then the parent(s) or legal guardian(s) consent should be sought and this may not always be appropriate. In Scotland, a child under 12 years old would be not be deemed competent to provide consent;

- As consent **must** be freely given, officers **must** consider how much choice would children or their parents (or legal guardians(s)) feel they have when the police are in attendance i.e. is there a power imbalance? (See Section 4.7.3, above).

4.7.10 Where Vulnerable Young People, Adults at Risk of Harm or Adults with Incapacity are concerned, information sharing based on consent as a Legal Gateway presents additional difficulties. The Adult Support and Protection SOP provides guidance in relation to use of the interim Vulnerable Person's Database (iVPD) and Divisional Concern Hubs where any doubt exists that the individual has the capacity to legitimately provide consent. The SOP provides procedural guidance on the implementation of the Adult Support and Protection (Scotland) Act 2007, which is further discussed in the Scottish Government's Adult Support and Protection (Scotland) Act 2007 - Code of Practice (particularly Section 10.13 'Capacity').

4.7.11 A lack of capacity to provide legitimate consent may also be derived from the subject having additional needs in areas such as:

- Communication skills;
- Attention span;
- Sensory impairment;
- The subject's first language being other than English;
- Any other relevant factors.

4.7.12 Where capacity to provide legitimate consent is limited due to the subject not having English as their first language, it may be possible to engage the services of an interpreter. The Interpreting and Translation Services SOP provides procedural detail on this; advising that, in informal (non-investigatory) settings, it may be acceptable to use the linguistic abilities of friends, family or neighbours. It should be noted, however that such resources should not be used when the information may be of a private or confidential nature (see Section 4.2, above – Common Law Duty of Confidentiality).

Note: It would normally be regarded as unacceptable to use police officers/staff who have sufficient linguistic skills to be able to translate, as this may adversely affect the balance of the relationship between subject and requestor (see Section 4.7.3, above).

4.7.13 If consent is the only appropriate Legal Gateway and cannot be obtained from the individuals themselves (either because of their age or capacity), consent can **only** be provided by a person who has the authority to act on behalf of that individual, i.e. welfare power of attorney or guardianship. If anyone other than this offers to provide consent, this could not be relied upon. Relevant documentation **must** always be checked to ensure the person has the correct authority. In this type of situation it may be more appropriate to obtain the consent in slow time rather than by the initial attending officers.

4.7.14 Due to the above requirements for ensuring that consent is properly sought and obtained, and the difficulties that may be encountered by requestors in legitimately obtaining consent, it is often advisable to explore whether a different Legal Gateway can be used.

4.7.15 If, however, consent is identified as the appropriate Legal Gateway for a proposed information sharing process, this should be documented in the associated ISA, detailing the process to be followed for obtaining and recording consent in an auditable format. Consideration should be given to whether valid consent can be obtained by frontline officers at initial point of contact with an individual, or whether it should/can be done in slow time.

4.7.16 The ISA should also document mechanisms for withdrawal (ensuring that individuals know how to withdraw consent), documenting any variations in consent and ensuring consent is refreshed when necessary. Records relating to consent should detail when and how the consent was obtained, exactly what the individual was told at the time and what they consented to.

4.7.17 If there is no associated ISA, an auditable record **must** still be kept detailing when and how consent was obtained, what the individual was told, what they consented to, evidence of the individual's consent, including any variations they have stipulated, (e.g. by notebook signature or telephone recording) and confirmation that advice was provided on how to withdraw consent.

4.8 Human Rights Act 1998

4.8.1 Any information which is shared **must** comply with the European Convention of Human Rights (part of UK domestic law via the Human Rights Act 1998). The right most likely to be infringed by information sharing is Article 8, the Right to Privacy.

4.8.2 The Right to Privacy is not absolute. However, a public body can only interfere under certain circumstances. Any information sharing, therefore**, must** be in accordance with the law (we **must** have a lawful basis for sharing), the interference **mus**t be necessary for the pursuit of a legitimate aim (for example the prevention and detection of crime or protection of health and morals) and **must** be proportionate (i.e. only share the minimum information required to meet that legitimate aim).

4.8.3 Any decision to share information should be on a case-by-case basis and document the purpose, the legal justification for sharing, and the necessity, relevancy and proportionality of the information shared. See Section 5 (below).

4.8.4 In particular, the risks to the individual's privacy by sharing the information, as well as the risk to the legitimate aim if the information is not shared, should be weighed against each other and documented.

5. Assessing Necessity, Relevancy and Proportionality

5.1 Once a potential Legal Gateway and a legitimate aim to interfere with the right to privacy have been identified, an assessment **must** be made regarding the necessity to share, and the relevancy and proportionality of the information to be shared. The judgment by the Supreme Court relating to the Information Sharing provisions of the Children and Young People (Scotland) Act 2014.

Note: The Christian Institute and others v the Lord Advocate (Scotland) (2016) UKSC 51 particularly emphasised the importance of this.

5.2 Necessity:

5.2.1 In order to justify that the information sharing is necessary, the rationale needs as a minimum to cover these points:

- The objective of the disclosure (e.g. outline the particular policing purpose or statutory obligation fulfilled), and the legitimate aim being pursued under the Human Rights Act 1998;

- The person whose data is being disclosed, and how they are linked to the policing purpose;
- The information being disclosed and how it relates to the policing purpose;
- The recipient organisation – do they have a statutory function for which the information is necessary? What action will they take, and is there reasonable belief that they will take this action?
- Confirm that there are no other reasonable means by which the recipient organisation could obtain the information, or that the policing purpose could be fulfilled;
- Consider and document whether the objective could be achieved without sharing personal data (e.g. could the data be anonymised?).

5.2.2 Where the identified purposes cannot be shown to be necessary, it is more likely that the lawful basis to be relied on is consent. However, consideration should be given to whether valid consent can be obtained, the other data protection principles can be complied with (e.g. compatible with original purpose for gathering, relevant, secure) and if not whether signposting would be an option, or not sharing at all.

5.3 Relevancy:

- The only information which can be shared is that which is relevant to the reason for the sharing. This **must** take account of the action to be taken by the recipient organisation. The information disclosed **must** be no more than that required for the recipient organisation to take action.
- It is a test of the relevancy and proportionality of the information held that sometimes leads to a decision not to share, or only to share part of the information requested (either by Police Scotland or by a partner agency).

5.4 Proportionality:

- Explain how the intrusion into privacy is justified when balanced against the benefits to the individual and/or society of the action taken by recipient organisation – any infringement of rights **must** be outweighed by the benefit;
- Could there be any unintended impact on another individual by disclosing the data?
- Confirm that the data has been minimised so that it is no more than is required to meet the objective of the sharing.

6. Recording of Decisions

6.1 Sharing of information **must** be on a **case by case** basis. If the guidance above is followed, a decision may be reached that information can be shared, but equally, it may be that after taking everything into consideration a decision is reached not to share. In either case, details of the decision and the rationale behind it **must** be recorded. This means that, in the event that the decision is subsequently challenged (e.g. as a result of a Significant Case Review (SCR), or Police Investigations and Review Commissioner (PIRC) enquiry, or a complaint from the data subject), the decision may be defended.

6.2 The following **must** be recorded:

- The rationale for sharing (or not sharing) the information (with reference to lawful basis, necessity and proportionality considerations outlined above);
- The date(s) the information was shared;
- The organisation(s) with whom the information was shared;
- Whether the information was provided in response to a specific request;
- If in response to a specific request, what information was requested and what information was ultimately shared;
- How the information was shared (e.g. electronically, hand delivery of hard copy, verbally at meetings);
- Whether the subjects involved were made aware and their views sought of the information being shared (to satisfy the data protection test of fairness), and if not, provide details as to why this was not done;
- If consent was required, confirmation of when and how obtained, who it was obtained from and what they were told, what information/recipient organisation is covered by the consent, where the auditable record is held

7. Information Sharing Agreements

7.1 ISA, ISPs and MOUs

7.1.1 A document which sets out a formal framework for the transfer of personal information between two agencies may commonly be referred to as an Information Sharing Agreement (ISA), Information Sharing Protocol (ISP) or a Memorandum of Understanding (MOU). ISAs and ISPs are just different names for the same type of document, however ISA is becoming the more commonly used terminology amongst public sector organisations.

7.1.2 For the purposes of the Police Scotland Record Set, the following terminology will be used:

- **Information Sharing Agreement** – ISAs are documents that describe and facilitate the legal and secure sharing of personal information (as defined within Data Protection legislation) between Police Scotland and one or more partner agencies. All ISAs will identify the legal gateway, (e.g. s139 of Antisocial Behaviour etc. (Scotland) Act 2004), the policing purpose (see 3.2, above) and support particular operational requirements.
- **Memorandum of Understanding** – MOUs are documents describing an agreement between two or more parties indicating a common line of action or agreed approach, and sets out in writing an understanding of the roles and responsibilities of the parties. Information may be shared as part of the agreement (e.g. guidance documents), but where Police Scotland is the author of the document, it will not include personal information as defined within Data Protection legislation.

7.2 Any information sharing which is frequent and systematic should be carried out within the framework of an ISA in order to ensure that information is shared legally and securely to the right person in the right place at the right time. Information Assurance should be contacted when a need for an ISA is identified, or to establish whether there is a need for an ISA. The ISA may apply one or more Legal Gateways as defined in Section 4 (above), either under the DPA 2018 or other specific legislation, but all ISAs will meet the principles embodied in the DPA 2018 (see Data Protection SOP for further guidance on the principles).

7.3 Having an ISA in place does not, in itself, provide a legal gateway for sharing. An ISA documents the risk assessment required to ensure that sharing can proceed more efficiently, e.g. the legal gateways, security requirements, breach procedures and information access rights will have been detailed in it. Each individual decision to share within the scope of an IAS must still be made on a case-by-case basis to ensure the necessity, relevancy and proportionality of the sharing, taking into consideration all the circumstances. The rationale behind the decision should be fully recorded.

7.4 Where an Information Sharing process is not linked to a legislative requirement or with a statutory partner agency (for example sharing with a TSO who provide support services), approval for the process should be sought from the Divisional Commander/Head of Department of the business area, and confirmation of this approval in writing must be supplied to Information Assurance.

7.5 ISA Register:

7.5.1 Where a need for an ISA is identified, Information Assurance must be contacted so that the details can be added to the Police Scotland Information Sharing Agreement Register, which is managed by Information Assurance.

7.5.2 The ISA register contains details of proposed, draft and signed ISAs and those under review. It also contains details of all partners, asset owners and Police Scotland Single Points of Contact (SPOC). It is mandatory that all Information Sharing Agreements are included on the Register.

7.6 Data Protection Impact Assessments:

7.6.1 When contacting Information Assurance to have the details of the ISA added to the register**,** advice should be sought as to whether a Data Protection Impact Assessment (DPIA) is required, if this hasn't already been considered.

7.6.2 Depending on the nature of the information sharing (for example where new technologies are being used, or there is a high risk to the rights and freedoms of individuals), it may be that a DPIA is required under the GDPR/DPA 2018.

7.6.3 DPIAs build on the principles which were formerly documented in a Privacy Impact Assessment (PIA). Similarly, a DPIA is a tool which can help an organisation identify the most effective way to comply with its data protection obligations and meet individuals' expectations of privacy. An effective DPIA will allow organisations to identify and fix problems at an early stage, reducing the associated costs and damage to reputation, which might otherwise occur. See the Data Protection SOP for further guidance.

7.7 Drafting an ISA

7.7.1 In circumstances where the information sharing process includes Police Scotland **sharing** as well as receiving information, Police Scotland **must** draft the agreement. If we are only **receiving** information, then the originating organisation **must** draft the agreement, and the recipient business area **must** liaise with Information Assurance to review the document and make any necessary amendments **prior** to signature.

7.7.2 A template containing the required headings and details of information management standards required is available from Information Assurance.

7.7.3 All ISAs **must** include the:

- Purpose of the ISA (business or legislative drivers – aims, strategic policing priorities met);
- Partners;
- Legal Gateway;
- Details of associated DPIA (if applicable) – risks identified and counter-measures applied;
- Fair processing information;
- Consent processes (if applicable);
- Circumstances in which sharing takes place;

- Nature of the information (including the Government Security Classification (GSC) marker applied – see Section 7.7.5);
- Means of sharing/receiving requests for information (consider email security, storage of information and how the process can be audited);
- Management of Information (including relevant protective markings and associated handling requirements, steps to ensure accuracy, procedures for secure disposal, restrictions on re-use, rights of individuals to access the information and security breach procedures);
- Retention (the relevant retention period **must** be identified and included);
- Training requirements (if applicable);
- Review Process (including post-holder with responsibility for the review, timescale, procedures and triggers for a review of the process);
- Signatories.

7.7.4 It can be helpful to draw up a process flow-chart of the information sharing mechanism that the ISA supports. Even simple flow-charts can identify 'pinch points', i.e. where extra security is required, where the Legal Gateway might change, or where a specific role may need to be developed. It will also help in any discussion you have with Information Assurance at any stage in the development of the ISA.

7.7.5 ISAs may be made available to members of the public and therefore should not contain any information in the body of the document which requires a protective marking above OFFICIAL. Any information which requires a higher protective marking, such as contact details, should be contained in the Appendices and given the marking OFFICIAL: POLICE AND PARTNERS. (See Section 9, below).

7.7.6 A process flowchart outlining the process used to establish an Information Sharing Agreement is provided at Appendix 'D'. This notwithstanding, Guidance can be obtained from Information Assurance at any time during the ISA drafting process.

7.8 Approval Process

7.8.1 Once the initial draft is complete, this should be submitted to Information Assurance, who will carry out an initial compliance check of the ISA. If the ISA is compliant then it can be shared with partners for their comments/amendments.

7.8.2 Once a final draft of the ISA is agreed upon, it should be re-submitted to Information Assurance for a final compliance check before being returned to the SPOC to arrange for the ISA to be signed.

7.8.3 When all partners have signed the ISA, the hard copy should be returned to Information Assurance for storage and inclusion on the ISA register. Where a partner other than Police Scotland holds the hard copy, an electronic copy of the signed document should be emailed to Information Assurance (see Appendix 'H') so that the ISA register can be updated.

7.9 Appropriate Signatories

7.9.1 If the agreement is between Police Scotland and another single national body, such as the Scottish Fire and Rescue Service, the document should be signed off by the Strategic Information Asset Owner (see Section 10.2, below) for that area of business (most likely at Assistant Chief Constable level), and an individual of corresponding position from the partner organisation.

7.9.2 If the document is between Police Scotland and an organisation local to a particular division, for example, a Local Authority or local National Health Service (NHS) Board, then it should be signed off by the local Divisional Commander, and an individual of corresponding position from the partner organisation.

7.9.3 Where an ISA is created in response to particular legislation (e.g. Prevent, Procurement Regulations), a general template agreeing the Legal Gateways and common standards can be drawn up and signed off by the relevant Strategic Information Owner, but individual ISAs can be signed off locally if relevant, allowing for variations in local processes.

7.10 Review of the ISA

7.10.1 New ISAs should be reviewed within six months of implementation, and yearly thereafter. These scheduled reviews will be instigated by Information Assurance, who will have a record of the review schedule contained within the ISA register. Information Assurance will contact the post holder with responsibility for the review process (detailed within the ISA) who will arrange for the review to be carried out and provide details of the outcome to Information Assurance.

7.10.2 The purpose of the review is to ensure that the ISA is achieving its purpose and that the sharing process is operating efficiently. As well as the ISA document itself, some of the information sharing transactions which have taken place should also be reviewed to ensure compliance with the legislation and the guidelines within this SOP.

7.10.3 It is the responsibility of the Operational Asset Owner to ensure that the review post holder undertakes the scheduled review, and in cases where the review post holder is the Operational Asset Owner, this responsibility would pass up to the Tactical Asset Owner.

7.10.4 However, a review may be triggered outwith the schedule by one of the following factors:

- An information security breach arising from the sharing arrangement;

- A complaint by an individual relating to the sharing arrangement;
- A change to the way that shared information is collected, recorded or managed by any of the partners to the agreement;
- Legislative change (e.g. a change to the statutory power underpinning the sharing arrangement

7.10.5 The factors above may be identified by any member of staff involved in the sharing arrangement, and they should contact Information Assurance and the post holder identified as responsible for the review process in order that the review can be instigated.

7.11 Information Request Forms

7.11.1 It is good practice to have a bespoke request form to cover information sharing between partners. Where a specific request form is to be developed to support an ISA process, the Forms Team within Policy Support should be consulted, and the form should be attached as an Appendix to the ISA. The forms will be published on the intranet as a Force Form.

7.12 Records of Information Requests/Information Shared under an ISA

7.12.1 Where decisions have been made to share under an ISA, the details **must** be recorded as detailed at Section 6 (above), and stored in accordance with any instructions contained within the ISA.

8. Requesting/Disclosing Information outwith an ISA

8.1 One-off or infrequent instances of information sharing can still take place, with the same principles outlined at Section 3 (above) taken into consideration. The same decision-making process detailed at Section 5 (above) should be utilised. Where an ISA exists the procedure documented therein should be followed.

8.2 Any information shared **must** be necessary, relevant and proportionate for the purpose for which it is shared (see Section 5, above). As detailed at Section 6.1 (above) it may be that, on balance, a decision will be made not to share, to refuse a request for information from another organisation, or only share/receive part of the information requested.

8.3 Information will not be shared where disclosure may compromise any police operation, investigation or initiative, or has the potential to cause harm to an individual.

8.4 Where intelligence is sought or intelligence is to be confirmed the National Intelligence Bureau (NIB) should be contacted. The NIB act as SPOCs for both requesting and sharing intelligence with organisations such as the Department of Work and Pensions (DWP, and Her Majesty's Revenue and Customs (HMRC).

8.5 Requesting Information outwith an ISA

8.5.1 There are a number of sections under the Data Protection legislation which provide a Legal Gateway for the release of personal information for specific policing purposes where the organisation the information is being requested from does not have Law Enforcement functions (e.g. a bank, shop, etc.) These are the sections relating to:

- Disclosure to the police for the purpose of safeguarding national security
- The crime and taxation exemption, which allows disclosure to the police for the:
    - Prevention or detection of crime
    - Apprehension or prosecution of offenders
- The lawful basis/conditions for processing which allow disclosure to the police to protect the vital interests of the data subject.

8.5.2 It would be very unusual for most police officers ever to use the Legal Gateway relating to national security; and vital interests should only be used in cases of life or death, such as where details of an individual are disclosed to the Ambulance service or a hospital's Accident and Emergency Department treating them after a serious road accident. The most common Legal Gateway for the release of personal information is the exemption for the prevention and detection of crime/apprehension or prosecution of offenders, under Schedule 2, Part 1, Section 2 of the DPA 2018 (which is the new equivalent to the more commonly known 's29 exemption', under the previous Data Protection Act 1998). Many organisations, and not just the Police Service, have commonly used a form to document the justification for the release of personal information, (see Force Form 052-003 - Requests for the Disclosure of Personal Data from External Organisations).

Note: If information is requested where the 'Vital Interests' of an individual is the Legal Gateway, the process is supported by Force Form 052-003A - Requests for the Disclosure of Personal Data from External Organisations (Vital Interests).

8.5.3 It is good practice that the reason for the request, giving sufficient detail to explain the necessity of the information to any investigation, is recorded on the form. The form **must** also detail the prejudice to the investigation should the information not be disclosed. This information is required to allow the receiving organisation to make an informed decision about whether or not the crime and taxation exemption applies. This gives an auditable record of the legitimacy of processing the information and is good practice suggested by the standards for compliance laid down by the Information Commissioner in their guidance on using the Crime and Taxation exemption.

8.5.4 Most organisations will require the written request to be countersigned by a supervisory officer of at least the rank of Inspector and there will often be a person, process or office within the organisation for dealing with such

requests. It is good practice to make enquiries about any process prior to making the request for personal information.

8.5.5 In emergencies most organisations will respond to a verbal request (where the identity of the person can be verified) for personal information but some form of audit trail should be provided at the time either by recording the request and the reason for it in the Police Officer's notebook or PDA and getting the entry and the response signed by the person providing the information or by countersigning the organisation's own file or record in the same way. Organisations will usually ask for a 'Request for Personal Data form 052-003' form to be provided as a follow up to this emergency process.

8.5.6 The exemptions which permit the release of information (further processing) under the DPA 2018 do not compel anyone to disclose information to the police and whilst many external bodies want to assist the police, they are often wary of doing so for fear that they breach the DPA 2018.

8.5.7 Pressure **must never** be put on individuals to comply with the request for information. Assistance or advice can be obtained from Information Assurance. (See Appendix 'H')

8.5.8 Copies of the request for information and the response received, **must** be retained as part of the disclosure (revelation) process for the crime or incident being investigated.

8.6 Disclosing Information outwith an ISA

8.6.1 If an information request is received where no ISA is in place, or it has been decided to share information/intelligence without a request, the following action **must** be taken:

- Where a request is received for information, the purpose for which the information is going to be used, the name, position, organisation, contact details of the person making the request **must** be obtained and recorded;
- The identity of the person making the request **must** be verified;
- Where information is shared proactively, the purpose for the sharing **must** be identified and recorded;
- A Legal Gateway (see Section 4, above) **must** be identified to allow the disclosure, or the individual **must** have consented. If not, then no information can be shared. If a request is made on the basis that a statutory power exists, the agency requesting the information **must** identify the legal power that allows them to lawfully request and process such information (for example, functions conferred on the organisation by legislation pertaining to their activities). Details of the Legal Gateway **must** be recorded. If there is any doubt as to whether the information can be disclosed, guidance **must** be sought from the relevant supervisor or Information Assurance;
- Record whether the subjects involved were made aware and if their views sought regarding the information being shared (to satisfy the data protection requirement of fairness);

- Use the decision making process outlined at Section 5 (above) to decide what is necessary, relevant and proportionate to share, and record the rationale;
- Details of the information requested, and if applicable, shared, **must** be recorded, including whether it includes personal or special category/criminal data (e.g. health information or convictions);
- The Legal Gateway which has been identified;
- If consent was required, record details of when and how consent was obtained, who it was obtained from, and what information/recipient organisation is covered by the consent;
- Where applicable, the signature of the authorising officer **must** be recorded (business areas should decide who the authorising officer will be for their own area).

8.6.2 Again, sharing of information **must** be on a case by case basis and whether a decision is made to share the information or not, details of the decision and the rationale behind it **must** be recorded. In the event that the decision is subsequently challenged (e.g. as a result of a Significant Case Review, PIRC enquiry, or a complaint from the data subject), the decision can be defended.

8.6.3 A flowchart detailing the process for sharing information outwith an ISA is shown at Appendix 'F'.

8.7 Further information on obtaining or disclosing information can be obtained from Information Assurance (see Appendix 'H').

8.8 Recording/Storage of Information Shared outwith an ISA

8.8.1 Records **must** be kept of information shared outwith an ISA (see Section 6, above). Electronic folders and files containing hard copies of documents should be controlled by the relevant business area, and managed in accordance with the Police Scotland Management of Records SOP.

8.8.2 A spreadsheet or similar should also be kept which details the decision making considerations in each case and this should be monitored by a supervisor. It will be subject to audit by Information Assurance and potentially the Information Commissioner's Office.

8.8.3 The spreadsheet should be reviewed regularly, and where requests to/from a particular organisation are assessed to be routine/frequent, consideration should be given as to whether an ISA is necessary.

9. Handling the Information

9.1 Transfers of information should be carried out as per the handling instructions in the Government Security Classification SOP.

9.2 Where possible, request forms/information to be shared should be sent to a secure email address. To be secure, e-mail addresses **must** contain one of the following: pnn, cjsm or NHS.Net. Otherwise additional security will be required in the form of a protective overlay or proprietary encryption. Consult Information Assurance or the Information Security Manager for further advice.

9.3 Many organisations, such as banks/building societies, do not have secure e-mail facilities. In such cases every effort should be made to submit the form by hand. If there is a requirement to share to an organisation that doesn't have secure email, consult with the Information Security Manager to see whether additional security can be obtained, e.g. by using software such as "Egress".

9.4 Transfers of information should only be posted to an organisation in exceptional circumstance and only if the proper recipient has been identified in accordance with the sensitivity of the information being transferred. The envelope should include a return address, however the classification should not be marked on the envelope. Consider using registered Royal Mail service or reputable courier with track and trace service. Official information with a descriptor must be sent by a trackable mail service. At OFFICIAL SENSITIVE double envelopes and a registered mail service must be used.

9.5 Information can be shared verbally in exceptional circumstances and where the identity of the person receiving the information can be verified, however a record of this and the reason for it must be recorded, and it must be followed up as soon as practicable in writing.

10. Roles and Responsibilities

10.1 All Staff

10.1.1 All staff have a responsibility to ensure that the sharing of information is done within the law and in line with this SOP. However, each person involved also has other specific responsibilities.

10.2 Strategic Information Asset Owners

10.2.1 Strategic Information Asset Owners (SIAOs) are the senior members of staff within the Force Executive who are responsible for a particular information asset (for example, a police system). SIAOs are responsible for understanding what information is held within their area of responsibility, what is created or added, how information is moved, who has access to it and why.

10.2.2 SIAOs are accountable for understanding and addressing risks to the information, and ensuring the confidentiality, availability and integrity of the information. Sitting beneath the SIAO are Tactical Asset Owners (Head of department or equivalent) and Operational Asset Owners (the role having day to day responsibility for the information asset).

10.3 Divisional Commanders/Head of Specialist Division (Tactical Asset Owners)

10.3.1 Divisional Commanders/Heads of Specialist Division have a responsibility for:

- Ensuring that an information sharing process is valid and necessary
- Supporting staff to share information appropriately
- Ensuring all ISAs for their business area are held centrally by Information Assurance
- Ensuring information sharing processes are adhered to by all staff and officers
- Authorising ISAs
- Ensuring ISAs are reviewed in line with Force Policy
- Ensuring staff involved in information sharing are appropriately trained

10.4 Supervisors

10.4.1 Supervisors have a responsibility for:

- Supporting staff to share information appropriately
- Ensuring information sharing responsibilities are included in the relevant job descriptions
- Checking by means of dip sampling, the decisions to share information made by their staff, in particular;
    - Whether the sharing is lawful
    - The necessity, accuracy, relevancy and proportionality of the information shared
    - Ensuring the sharing does not compromise any police operation or the safety of others
    - Ensuring a risk assessment has been carried out on any information shared
    - That the information shared has been recorded correctly.
- Checking by means of dip sampling, decisions made refusing to share information
- Providing feedback to staff on their performance on an ongoing basis

10.4.2 As a guide, it is recommended that one percent of all decisions (with a minimum of five where 1% is less than five) be checked each month.

10.4.3 Details of these checks should be recorded and the results available to the individual in order that any learning points can be identified.

10.4.4 Records of these checks **must** also be available to Information Assurance for audit purposes.

10.5 Owner/Reviewer

10.5.1 The owner/reviewer of the ISA is the person who is responsible for:

- Developing/designing the process and/or has the organisational oversight of the activity;
- Ensuring the drawing up of any Standard Operating Procedure (SOP) that may be required to accompany the ISA;
- Ensuring that the ISA remains up to date and fit for purpose;
- Ensuring completion of the Equality and Human Rights Impact Assessment;

  and

- Working with an Information Assurance Officer to ensure governance and legal compliance.

10.5.2 The role of the owner will be identified in the section of the ISA that describes how the process and the agreement is reviewed by the partners to the agreement.

10.5.3 The owner and reviewer may be two separate people; one with initial ownership of the process and a subsequent reviewer. This should be outlined in the ISA. Should substantive changes to the ISA be required, however, an owner **must** again be identified.

10.5.4 All ISAs will be reviewed yearly, however if circumstances or processes change before then, it is important that the ISA is brought up to date. Practices not based on a SOP, ISA or other guidance document may mean that information is being shared irregularly and therefore illegally and will be open both to internal and external challenge (see Section 6.1, above).

10.5.5 It should be noted that ownership of the ISA belongs to the role and not the individual.

10.6 Author/Lead Practitioner

10.6.1 The Tactical or Operational Asset Owner will appoint an author/lead practitioner who will act as a single point of contact (SPOC), liaising with partners and consulting with others, including Police Service Policy Leads, as necessary to prepare a draft ISA. An Information Assurance Officer appointed by the Information Assurance team within Information Management should be involved in this process.

10.6.2 The author/lead practitioner, in conjunction with the owner, is responsible for ensuring an Equality and Human Rights Impact Assessment is conducted, and any issues identified are brought to the attention of the Owner.

10.6.3 The author/lead practitioner is also responsible for ensuring that approval is sought from Divisional Commander/Head of Specialist Division where necessary.

10.7 Users

10.7.1 Users are responsible for:

- Applying Force policies, procedures and guidance relating to information sharing;
- Ensuring that the sharing of information is lawful and the requirements of the DPA 2018 and the common law duty of confidence have been fulfilled;
- Ensuring that the information being shared is accurate, relevant, proportionate and necessary for the purpose for which it is being shared;
- Recording in accordance with this guidance, any decision to share/not share information.

10.8 Information Assurance

10.8.1 Information Assurance should be contacted in every instance where an ISA is to be developed. Information Assurance will be responsible for:

- Providing advice and guidance (and where required, training) on information sharing, including the appropriate legal framework and the development of the ISA and associated processes;
- Quality assuring ISAs before they are issued for wider review (e.g. by partner agencies) or arrange for the compliance checking of all ISAs and accompanying SOPs (if required), where possible by staff other than those who have been involved in giving advice;
- Auditing the sharing of information both through and outwith ISAs;
- Ensuring this SOP is kept up to date and for development of such other guidance as may be required.

Note: Information Assurance is **not** responsible for making information sharing decisions.

10.8.2 Information Assurance will also be responsible for:

- Maintaining the register of ISAs under development and tracking their progress from initial query to conclusion;
- Maintaining a central repository of Police Scotland's ISAs;
- Recording files registered to individual ISAs (e.g. bespoke request forms);
- Ensuring all ISAs are published on the intranet;
- Ensuring a programme of review of all ISAs;

10.8.3 After initial compliance checking by an IAO, the draft may be circulated to other parts of the Service who may be interested in developing similar agreements (subject to minor local process variations).

10.8.4 Once the compliance process is completed the IAO will return the ISA to the SPOC who will arrange for the appropriate signatory/Partners to sign it. The master copy of the ISA and an electronic scanned copy will be returned to the IAO to update the Information Sharing Agreement register to reflect that the document is signed, and arrange for a copy to be uploaded on the Intranet. It is expected that most ISAs will also be uploaded on to the external Police Scotland website via the Publication Scheme.

10.8.5 The IAO may arrange for audits of processes to be carried out to ensure that all are compliant.

10.9 Legal Services

10.9.1 In most cases, Legal Services will not need to be consulted during the ISA drafting process. However, on some occasions they may be consulted to clarify a point of legislation, or where an ISA has been drafted by a partner agency and contains legal clauses.

10.9.2 Engagement with Legal Services relating to an information sharing process should be done in conjunction with Information Assurance so that both operational/business needs and compliance issues can be considered.

11. Further Advice and Guidance

11.1 Further advice and guidance in relation to the contents of this SOP can be obtained by contacting the Information Assurance department (see Appendix 'H').

Appendix 'A'

List of Associated Legislation

- General Data Protection Regulation (GDPR);
- Data Protection Act 1998 – now repealled
- Data Protection Act 2018 (DPA 2018);
- European Union Data Protection Directive 2016/680;
- Human Rights Act 1998;
- Antisocial Behaviour etc. (Scotland) Act 2004;
- Children's Hearings (Scotland) Act 2011;
- Police and Fire Reform (Scotland) Act 2012;
- Adult Support and Protection (Scotland) Act 2007
- The Police Act 1997;
- Counter-Terrorism and Security Act 2015;
- Children and Young People (Scotland) Act 2014

Appendix ‘B’

List of Associated Reference Documents

Policies

- Data Protection
- Information Security
- Records Management

Standard Operating Procedures

- Data Protection SOP;
- Management of Records SOP;
- Government Security Classification SOP;
- Adult Support and Protection SOP;
- Interpreting and Translation Services SOP

Guidance

- Adult Support and Protection (Scotland) Act 2007 - Code of Practice

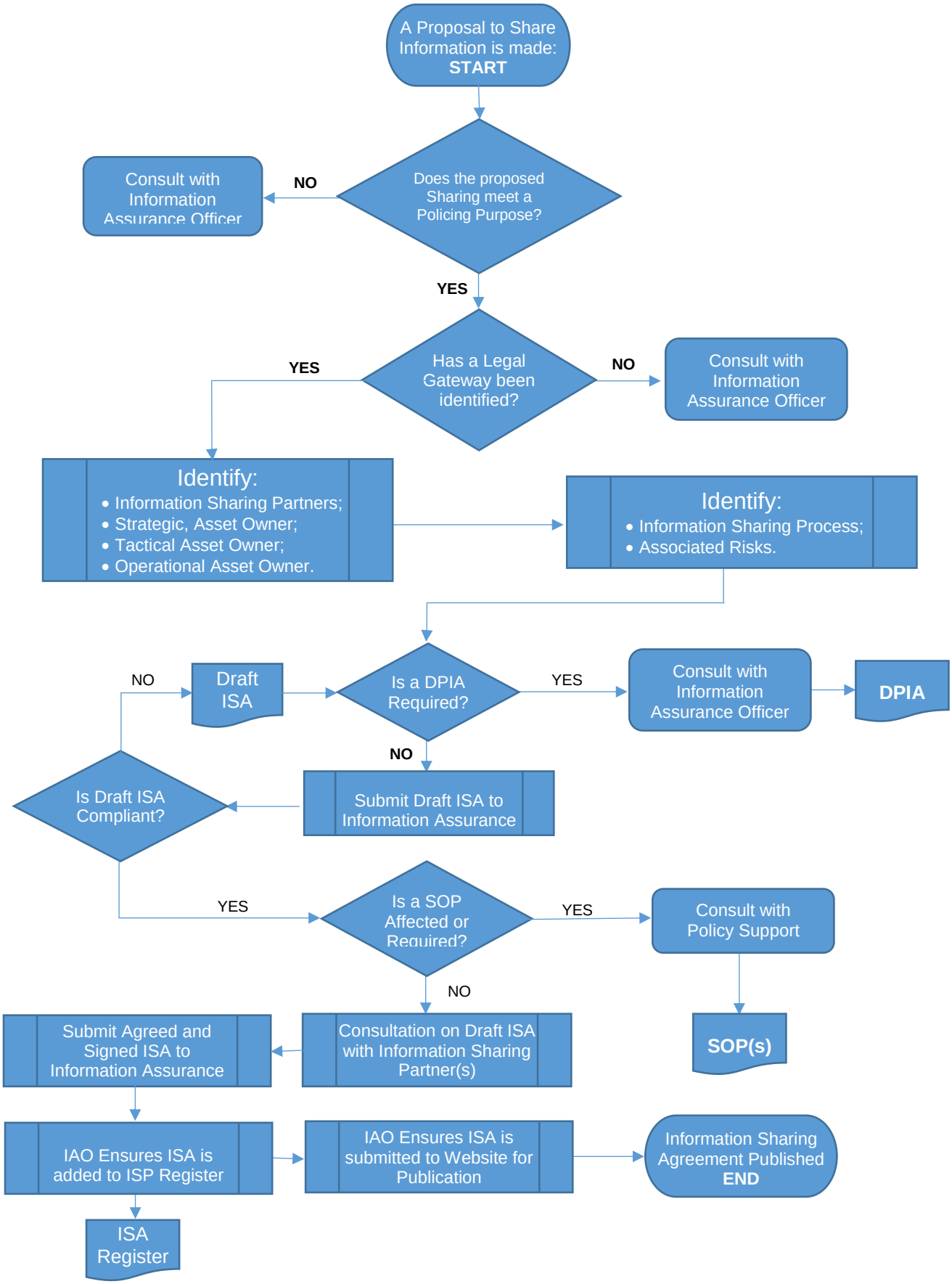
Appendix ‘C’

List of Associated Forms

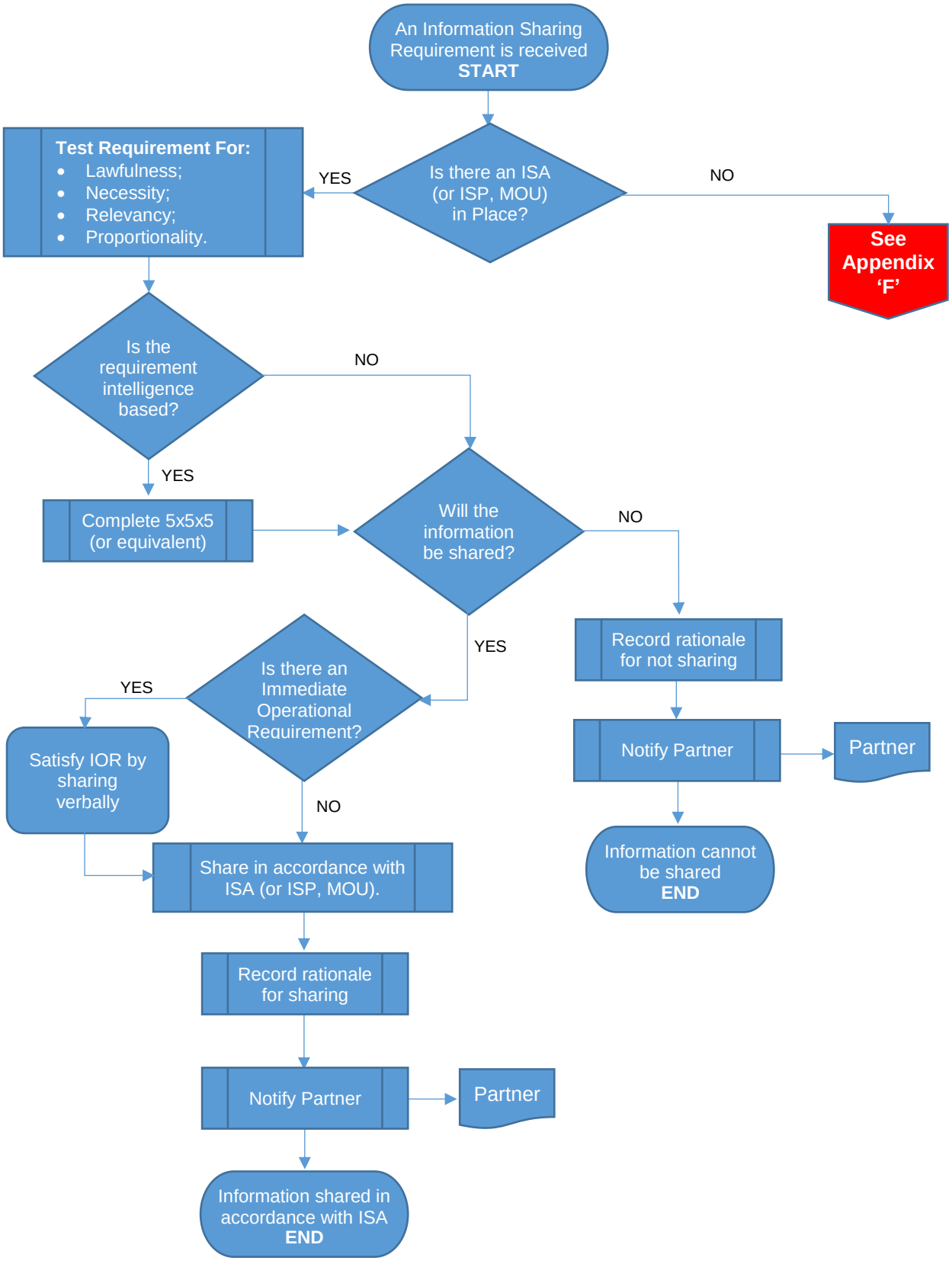
- Force Form 052-003 - Requests for the Disclosure of Personal Data from External Organisations.

- 052-003A - Requests for the Disclosure of Personal Data from External Organisations (Vital Interests).

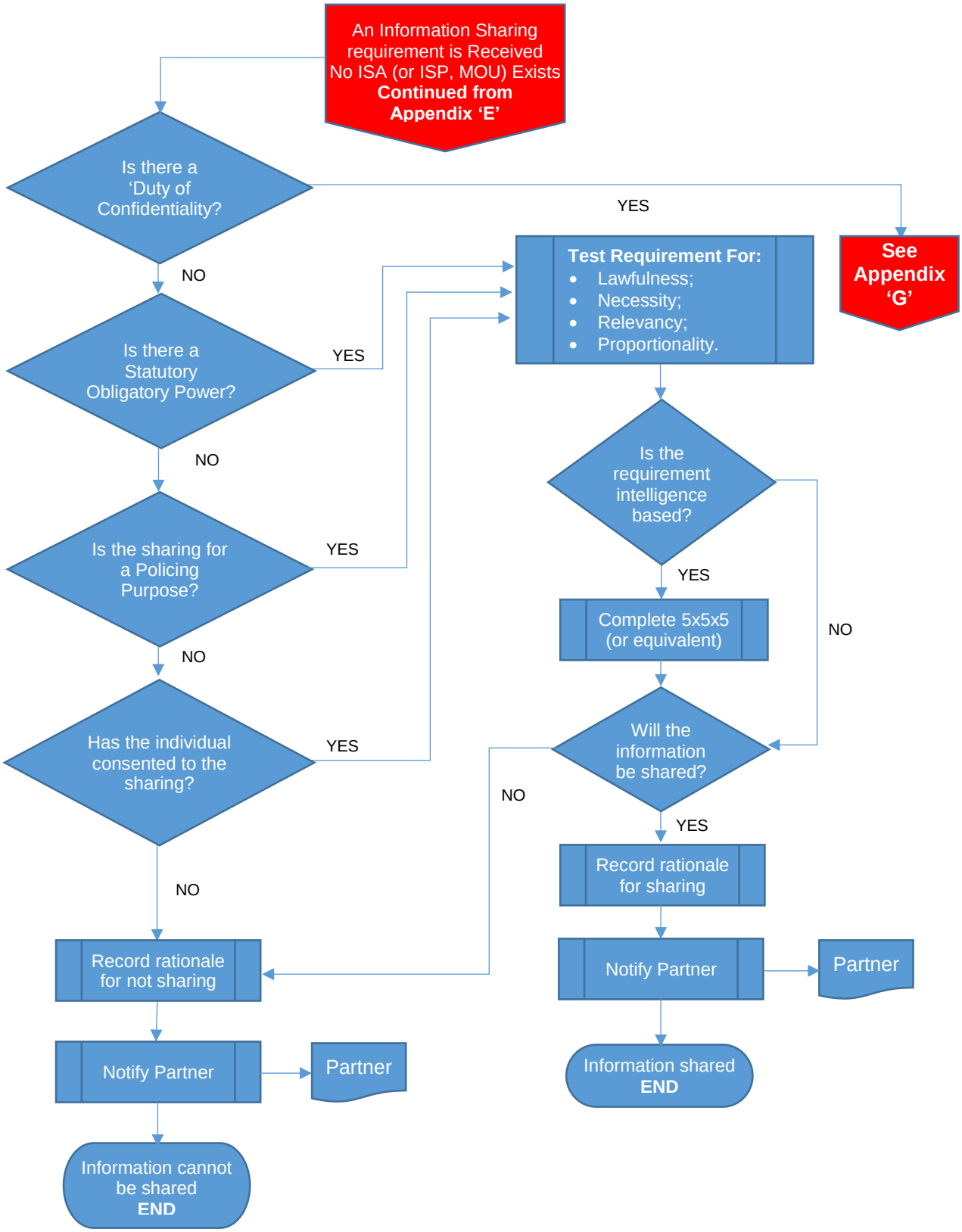
Information Sharing Agreements – Process Flowchart



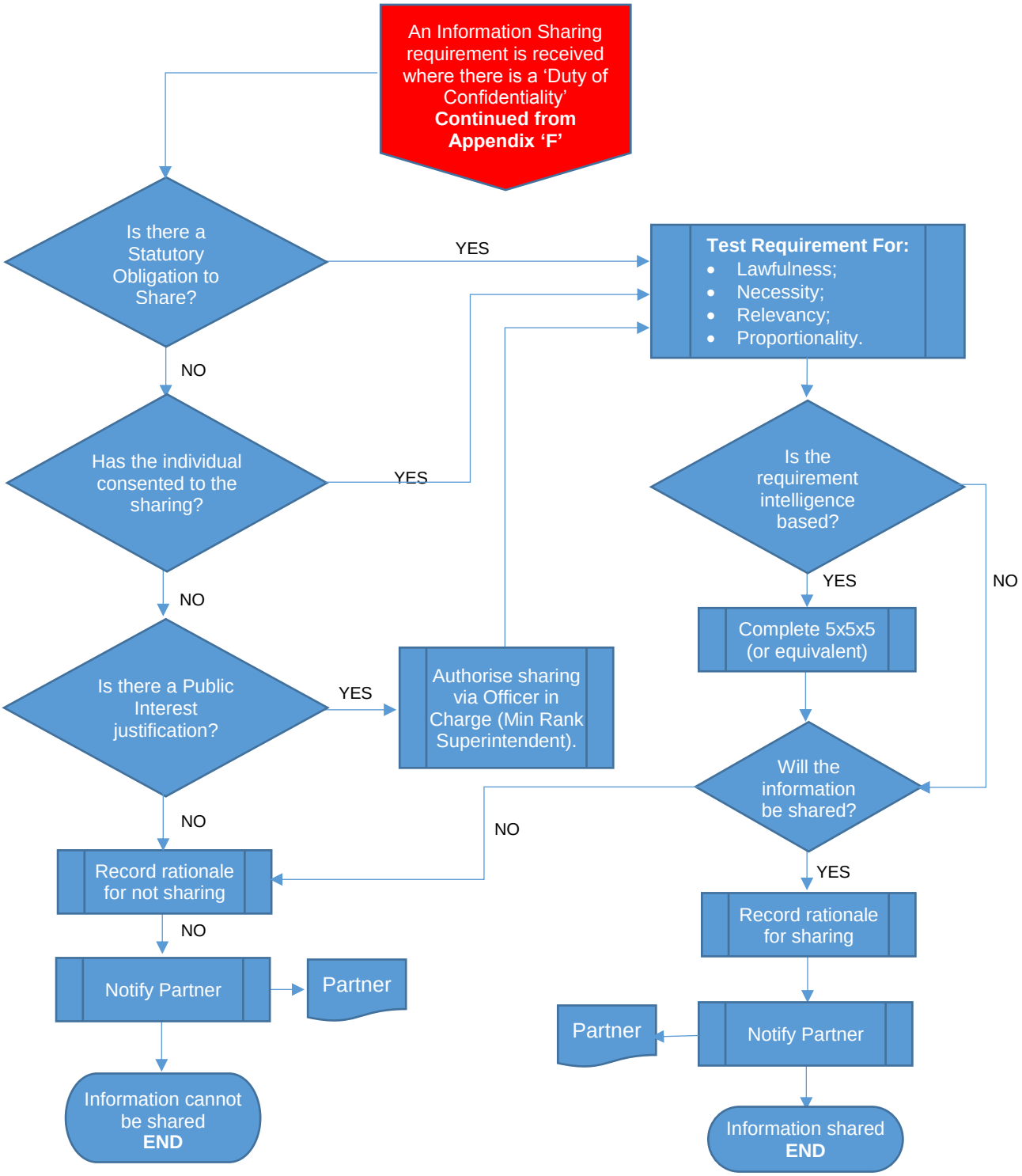
Information Shared as part of an Information Sharing Agreement Process Flowchart



Information Shared outwith an Information Sharing Agreement Process Flowchart



Information Shared where there is a 'Duty of Confidentiality' Process Flowchart



Appendix 'H'

Contact Details

Information has been removed due to its content being exempt in terms of the Freedom of Information (Scotland) Act 2002, Prejudice to Effective Conduct of Public Affairs.