Devon & Cornwall Police

Building safer communities together

AGREEMENT FOR THE EXCHANGE OF INFORMATION IN RELATION TO SAFEGUARDING ADULTS IN DEVON, CORNWALL AND THE ISLES OF SCILLY

VERSION 2.0

JULY 2015

Contents to be added

AGREEMENT FOR THE EXCHANGE OF INFORMATION IN RELATION TO SAFEGUARDING ADULTS IN DEVON, CORNWALL AND THE ISLES OF SCILLY

1 PURPOSE

1.1 The purpose of agreement to share personal data is to;

- Provide assistance, via the exchange of information, to adults with care & support needs/adults at risk or vulnerable persons who;
  - fit the criteria of the Care Act 2014
  - are experiencing or at risk of abuse
  - are at risk of neglect
  - may compromise the safety of themselves or others.
- Provide a method of exchanging information at Strategy Meetings or discussions, at scheduled Multi-Agency Safeguarding Adult Case Conferences, or promptly via formal request and disclosure forms.
- Ensure that vulnerable persons who are adults that may be the subject of vulnerability forums/meetings who will not necessarily 'fit' the criteria of the Care Act (not having care and support needs and are not at risk of abuse or neglect).
- To assist joint working for the purposes of safeguarding adults, responding to reported incidents of abuse, and the investigations and detection of criminal or unlawful acts and anti-social behaviour committed against adults with care & support needs/adults at risk or vulnerable persons.
- Assisting a SAB in relation to Safeguarding Adult Reviews (SAR's).

1.2 This agreement whilst seeking to promote multi agency working accepts that disclosures for the purposes given in 1.1. above will be dealt with utilising a power to disclose as opposed to an absolute duty to disclose.

1.3 This agreement also covers partnership working to enable partner agencies to identify risk and any un-met needs. Referrals to another partner agency who offer support and assistance outside of the purposes given in 1.1 above will take place with the knowledge and consent of the individual. Consent wording is given at Appendix 6.

2 PARTIES/SIGNATORIES

Devon and Cornwall Police

Cornwall Council

Cornwall Partnership NHS Foundation Trust

NHS Kernow CCG

NHS England/ Devon Cornwall and Isles of Scilly Area Team

Council of the Isles of Scilly

Devon County Council

Devon Partnership NHS Trust

Northern, Eastern and Western Devon CCG

Northern Devon Healthcare NHS Trust
Plymouth Community Healthcare CIC
Plymouth City Council
Plymouth Hospitals NHS Trust
Royal Devon & Exeter Foundation NHS Trust
Royal Cornwall Hospitals NHS Trust
Torbay and Southern Devon Health and Care NHS Trust
Torbay Council
South Devon Healthcare Foundation Trust
South Devon and Torbay CCG

2.1 The Partners within this agreement subscribe to the following: -

- the agreed standards must provide safeguards and an appropriate framework for the controlled exchange of timely, accurate and relevant information.
- the Data Protection principles and the common law principles of confidentiality must be upheld.
- the rights of the Data Subject under The Human Rights Act 1998 and particularly Article 8 of the European Convention on Human Rights are to be upheld within this agreement.
- this agreement to be reviewed annually, or in the light of new legislation or guidance.
- any partner may request any change to the agreement at any time by submitting to the agreement holder a suggested revision
- the nominated holder of this agreement is the Data Protection Officer, Devon and Cornwall Police, who shall, on behalf of the partnership:
    - ensure that a review is carried out in the first six months of the document being signed and then subsequently reviewed on an annual basis
    - circulate all requests for change, co-ordinate responses, obtain agreement for the changes from the partnership and distribute codes of practice and guidance as these become available;

2.2 Appendix 7 contains the contacts that should be referred to in each organisation.

3 DEFINITIONS

3.1 A “Data Subject” within this agreement will be an adults with care and support needs/adult at risk or vulnerable person, or the suspect of any alleged misconduct.

Safeguarding duties apply to an adult who; has needs for care & support (whether or not the local authority is meeting any of these needs) and; is experiencing, or at risk of, abuse or neglect; and as a result those care & support needs is unable to protect themselves from either the risk of, or the experience of abuse or neglect).

3.2 For the purpose of this agreement the term:

“Abuse” includes physical abuse, sexual abuse, psychological abuse, financial or material abuse, neglect or acts of omission, discriminatory abuse and institutional abuse (from 1 April 2015 “Abuse” includes domestic violence, modern slavery, organisational abuse & self-neglect).

"Anti-social behaviour" means acting in a manner which causes or is likely to cause harassment, alarm, or distress to one or more persons who are not of the same household as the identified person.

"Crime" is defined as any act, default or conduct prejudicial to the community, the commission of which by law renders the person responsible liable to punishment by a fine, imprisonment, or other penalty.

"Disorder" is an expression that refers to the level or pattern of anti-social behaviour within a particular area.

“Personal data” is information that relates to a living individual who can be identified from that data, or from the data and other information which is in the possession of or is likely to come into the possession of the data controller. It includes any expression of opinion or intentions in respect of the individual.

“Sensitive Personal Data” is Personal Data consisting of information as to-

(a) the racial or ethnic origin of the Data Subject,
(b) his/her political opinions,
(c) his/her religious beliefs or other beliefs of a similar nature,
(d) whether he/she is a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992),
(e) his/her physical or mental health or condition,
(f) his/her sexual life,
(g) the commission or alleged commission by him of any offence, or
(h) any proceedings for any offence committed or alleged to have been committed by him/her, the disposal of such proceedings or the sentence of any court in such proceedings;

“Data owner” is a person or organisation who controls the purposes, contents and use of personal data.

"Data controller" means a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed.

4 DETAILED STANDARDS

4.1 Scope

This agreement will cover the exchange of information between the nominated officers or authorised deputies with the partner agencies and will relate only to persons living or incidents occurring in the counties of Devon and Cornwall.

4.2 Registration/Notification

Each partner will ensure that they are appropriately registered under the Data Protection Act to receive and process personal data.

Data to be transferred will include some sensitive personal data. It will be necessary, therefore, to select criteria for processing from Schedules 2 and 3 of the 1998 Data Protection Act.

4.3 Legal Issues

It is essential that adequate control of the flow of data be maintained. The 1998 Data Protection Act permits the processing of data provided the data has been fairly obtained and processed (the individual has been clearly informed how their data will be used and disclosed), and it is appropriately notified under the Act. However, disclosures can also take place under certain circumstances, where the data protection principles will not apply - under the Act's non-disclosure provisions. Reliance on these must be assessed on a case by case basis. The provisions include:-

- At the request of and with the consent of the individual concerned, or making a best interest decision under the Mental Capacity Act 2005, as they are incapable of understanding the request.
- To protect the vital interests of the individual where consent cannot be given or is withheld
- For the prevention or detection of crime, the apprehension or prosecution of offenders. Disclosure of pertinent and relevant information must be on a case by case basis and where failure to provide the information would be likely to prejudice these purposes. Disclosures under this provision which are made pursuant to the prevention or detection of crime will only be made when the criminal act in question is relevant to the objectives of this agreement, namely safeguarding adults at risk. Further, for this provision to apply there would have to be a substantial risk of prejudice. All requests and responses must be appropriately authorised and documented.
- Where a disclosure is made in connection with legal proceedings, for the purpose of obtaining legal advice, and establishing, exercising or defending legal rights.

Further details of the legal provisions to support information sharing under this agreement can be found at Appendix 3- Legal Issues

4.4 **Handling of requests and disclosures.**

Procedures for the handling of disclosures of, or requests for, information can be found in;

- Devon -Safeguarding Adults Multi-Agency Policy & Procedures working guide, or
- Cornwall & Isles of Scily – Multi-Agency Safeguarding Adults Policy, April 2010 or
- Torbay -Safeguarding Adults Multi-Agency Policy & Procedures working guide or
- Plymouth-Safeguarding Adults Multi-Agency Policy & Procedures working guide.

4.5 **Disclosures made at meetings**

- Partner representatives, who anticipate making disclosures at Safeguarding Adults strategy meetings and Case conferences, should ensure they are empowered to do so and that proposed disclosures are covered by the relevant legislation. Such disclosures should be recorded within the minutes of the meeting. These minutes will be owned by the relevant Safeguarding Manager and must be retained for at least six years.

- Strategy Meetings, will normally only be attended by Statutory Agencies. However, in the event of another non statutory party being present at a strategy meeting, or attending Multi-Agency safeguarding Adult Case Conferences the chair and Multi Agency group should discuss whether pertinent information can be shared, based on the level of risk according to the provisions i.e if there is significant risk disclosures. This decision will be made whilst these parties are excluded. Where it is agreed that a disclosure will be made for example to a Care Home Manager, the disclosed data and the reasons for the disclosure should be documented and recorded in the minutes. However, in specific cases of disclosure of criminal convictions, it may be decided, as based on a reduced level of risk, that the other party be advised to undertake a further DBS check.

- Partner representatives who anticipate making verbal disclosures at other Information Sharing meetings should ensure they are empowered to do so and that proposed disclosures should be matters of fact and any opinion clearly stated as such. Information Sharing/Professionals meetings at local areas are likely to include discussions regarding frequent users of multi agency services, to identify risk and to identify any un-met needs. Where these meetings agree that support can be offered to an individual, the individual will be contacted by the partner organisation where they first came to attention to offer support and assistance and to sign the consent to share information form (Appendix 6). There may be occasions where consent is not appropriate or not given, under these circumstances a lawful basis to share without consent must be identified and documented.

- It is recommended, as a model of good practice, those attending such meetings should clarify all issues relevant to disclosure, to include

confidentiality and the disclosure powers which exist, prior to the commencement of the meeting. Regarding the police, if there is a forseeable issue concerning disclosure, advice and authorisation should be sought from the Police Public Protection Unit Detective Chief Inspector.

4.6 Disclosure under Direct Payments Schemes

Users of direct payments schemes may be at increased risk of abuse. In line with the Police Act 1997 and HO Circular 5/2005, whilst care workers employed in care homes are required to undergo Disclosure and Barring Service (DBS) checks, personal assistants who are employed by adults who have care and support needs through the Direct Payments Schemes are not required by law to be police checked through the DBS. As service users cannot instigate these checks themselves the service user should be encouraged to ask Social Services Depts to carry out enhanced DBS checks for proposed direct personal assistants and to await the outcome before employing a personal assistant.

As the service users cannot instigate checks themselves, the disclosure as a result of the DBS check should only consist of 'suitable' or 'not suitable' for Direct Payments. Personal assistants are sent a copy of the result of their own DBS check, therefore, they have the opportunity to dispute or challenge any of the information it contains and would be able to show the service user their own document if they wished. Under the Disclosure & Baring Scheme personal assistants are at present excluded from the registration process and therefore it is imperative that service users are encouraged to request checks.

4.7 Disclosure and Barring Service (DBS)

The Disclosure and Barring Service (DBS) helps employers make safer recruitment decisions and prevent unsuitable people from working with vulnerable groups, including children. It replaces the Criminal Records Bureau (CRB) and Independent Safeguarding Authority (ISA).

The DBS are responsible for:

- processing requests for criminal records checks
- deciding whether it is appropriate for a person to be placed on or removed from a barred list
- placing or removing people from the DBS children's barred list and adults' barred list for England, Wales and Northern Ireland

Referrals are made to the DBS when an employer or organisation, e.g. a regulatory body, has concerns that a person has caused harm, or poses a future risk of harm to vulnerable groups, including children.

In these circumstances the employer must make a referral to the DBS, though this is not obligatory for regulatory bodies.

For more information about the DBS see https://www.gov.uk/government/organisations/disclosure-and-barring-service/about#referrals

In the case of statements made to the police, informed consent must be sought in order to share statements supplied by individuals for their evidence to be used as part of this process. A tick box on the reverse of the MG11 is not deemed sufficient (see FAQ's page 17 in relation to case documentation).

For other disclosures from police records, the Force Public Protection DCI's advice and authorisation should be sought.

Source:https://www.gov.uk/government/organisations/disclosure-and-barring-service/about#referrals 23 April 2014

4.8 **Nomination of Staff**

In order to comply with the principle of security and the common law duty of confidentiality, this agreement contains a list of appropriate nominated officers or authorised deputies (see Appendix 3 – Partners to supply this information)

- With whom contact should be made in relation to disclosure of information under this agreement
- To whom requests for information should be sent.
- To whom disclosures should be made

Requests from unauthorised organisations/staff will be declined. Disclosure of information from Health partner agencies must be endorsed by the relevant Caldicott Guardian unless the relevant Signatory notifies the Nominated Holder otherwise.

Any changes in responsible officers will be notified to the Agreement Holder, in writing.

4.9 **Accuracy of Data**

Each partner has a responsibility to maintain the accuracy of data supplied under this agreement. There is a statutory duty in the 1998 Data Protection Act on a partner supplying personal data to verify the information and advise the recipients if the data supplied is subsequently found to be inaccurate.

Where an inaccuracy is discovered, after a disclosure has been made, it will be the responsibility of the party discovering the inaccuracy to bring this to the notice of the data owner, in writing, who should notify all recipients of the correction.

To meet this responsibility, partners are expected to record disclosures to indicate that a disclosure has been made and to inform recipients if they become aware of any inaccuracies which may prejudice the rights and freedoms of the data subject or individual, or detrimentally affect them.

4.10 **Confidentiality, Security and Retention/Disposal of Data**

Each partner organisation shall at all times keep confidential all personal data supplied pursuant to this agreement. This clause shall survive termination of the agreement or the withdrawal of or removal of any partner. Any resultant publication of data supplied pursuant to this agreement, related to the multi agency working for non-partner circulation, will not identify any individual.

Each partner will take all reasonable steps to adequately protect the data from both a technological and physical point of view, and this includes manual files and transfers of data between partners. The Police will grade the information provided to them, to restrict access, where this is applicable

One of the principles within Data Protection legislation states that excessive data must not be retained. It follows that data must be removed as soon as it is no longer required for the original purpose for which it was supplied or collected. To achieve this, partners are expected to introduce a procedure and nominate a person to conduct reviews at a cycle not exceeding six monthly.

All information subject to this agreement must be disposed of securely at the end of the retention period. Electronic forms of the information must be disposed of securely using a security accredited method of deletion. This includes any copies of the data which has been backed up or copied off site.

All paper forms of the information must be securely shredded. The costs of disposal will be met by the data processor.

4.11 **Breaches**

Any breach of confidentiality, or incident, involving a risk or breach of the security of information should be notified to the designated Data Protection/Information Assurance Manager of the relevant organisation without delay to ensure this is dealt with in accordance with their respective policy, procedures and the indemnity for this agreement.

If any information which is shared under this agreement is lost, stolen, or disclosed to anyone who should not have had access to it, this shall be a breach of this agreement.

The Data Controller for the breaching party must notify the other party of any breach by the breaching party as soon as it becomes aware of the breach. If there is suspicion of a breach, this also must be notified immediately.

Investigation into the breach will be conducted by the Data Controller for the breaching party. All investigation information will be shared with the Data Controller for the non-breaching party. Each Data Controller reserves the right to appoint their own investigating authority. The Data Controller and Data Processor of the breaching party will cooperate fully with any independent investigating authority.

4.12 **Data Subject Requests**

Individuals have the right of access to a copy of all information held about them on computer and manual files – unless an exemption applies where information can be withheld under certain circumstances. Partners will adopt common procedures for dealing with information access requests. See Appendix 4 for procedures on handling requests for individuals' access to information.

4.13 **Complaints**

Any complaint made will be brought to the attention of the nominated officer of the relevant partner, and they will be dealt with in accordance with their own policies

and procedures. Partners will keep each other informed of developments following a complaint received, where relevant.

4.14 **Compliance and Good Practice**

Any further guidance or codes of practice should be reviewed annually and distributed via the agreement holder for consideration and possible attachment to this agreement.

4.15 **Equality Act 2010.**

The assessment of relevance and impact of this agreement in relation to the public authorities' general duty under the Equality Act is the individual responsibility of the signatories

4.16 **Publication of Agreement**

This agreement may be published by each of the Signatories in accordance with their respective obligations under the Freedom of Information Act [FoIA] 2000. No section of the agreement is currently classed as 'Closed' under Freedom of Information.

The 'Durant' ruling of the Court of Appeal (Civil Division) in December 2003 has indicated that, in relation to this agreement, data linked to an individual's role, e.g. role title and contact number is not 'personal information'. Therefore the contact details of each Contact and Nominated Officer quoted within Appendix 7 will be published within the agreement under FoIA.

5 INDEMNITY

5.1 By signing up to this agreement, each partner shall be fully indemnified by the other partners in accordance with the following:

The parties hereto are working in partnership in exercise of their functions and their responsibility for the protection of the public

1. This agreement provides guidance on the exchange and use of personal information.
2. Further the parties have agreed to indemnify one another in the manner described below in circumstances where a person who is the subject of information exchanged between any of the parties in accordance with the agreement suffers loss as a result of the misuse or inaccuracy of the information and brings an action claim or demand as a consequence thereof.
3. In respect of the indemnity the parties have agreed as follows:-

Provision of Information
In consideration of the provision of information in accordance with this agreement the parties hereby undertake to indemnify and keep indemnified each other against all loss damages or liability (whether criminal or civil) costs charges and expenses including legal fees and costs at any time incurred or suffered by a party to this agreement arising on or out of the misuse of information provided in

accordance with the agreement. Provided that such indemnity may only be invoked in the circumstances set out in sub-clauses (a) to (d) below.

a) The party seeking the indemnity may only seek to enforce it against the party that supplied or misused the information in accordance with this agreement.

b) The party claiming the benefit of the indemnity has notified the party against whom it intends to invoke the indemnity within 14 days of any third party action claim or demand ("the claim") and thereafter the parties shall consult as to how the party against whom the claim has been made ("the defendant") should proceed in respect of such claim.

c) In the absence of contrary agreement between the parties the defendant shall resist the claim as far as final judgement. In the event of any claim being paid or compromised or in the event of final judgement being given against the defendant, the party against whom the indemnity is being invoked will within 14 days of being so notified by the defendant reimburse the defendant with the full amount of such payment or final judgement payment such payment to cover those costs and expenses identified in 3 above. Provided always that where any claim is paid or compromised the party against whom the indemnity is being invoked shall have the right to be consulted as to the extent of any payment.

d) The party seeking to invoke the indemnity may not do so if it has made or makes any admission which may be prejudicial to the defence of the action claim or demand.

6 CERTIFICATION –AGREEMENT FOR THE EXCHANGE OF INFORMATION, IN RELATION TO SAFEGUARDING ADULTS IN DEVON AND CORNWALL

By signing below, the participants accept and will adopt the statements included in this agreement and the indemnity, and agree to maintain the specified standards. In addition, the partners will not use, release or otherwise disclose any data whatsoever

- for any other secondary use; and/or
- to any organisation which is not a signatory to this agreement.

Signed ……..

Name and position of person signing ……

for and on behalf of (Organisation) ……

Date ……

7 REVISION INFORMATION

Version No	Date of Version
Draft June10.	Complete revision based on 2002 agreement
Working version 1.0 December 2010 Jan 2011 Feb 2011 March 2011 Oct 2011	Amendments made to; Throughout – protocol replaced with agreement – plain English. Section 2: Added Royal Devon & Exeter NHS Foundation Trust and South Devon Healtcare NHS Foundation Trust Section 4.6: Disclosure under Direct Payments Schemes - Amended text re personal assistants. Appendix 1 – text added re use of remote secure access to information. Section 3: Revision from Devon NHS to Torbay Care Trust as request of Care Trust Appendix 3: Contact Details inserted for Torbay Care Trust. Amendments requested by Devon County Council Amendments at Sections; 2, 4.4 and Appendix 3 requested by Cornwall Council NHS Devon contact details updated Torbay Care Trust contact details updated Sect 4.4. Page 7. Add April 2010 to the Cornwall & Isles of Scilly Multi-Agency Safeguarding Adults Policy Taken out Probation Service as signatory. Sent to Plymouth Council, Torbay Care Trust, R D & E NHS Foundation Trust, S Devon Healthcare NHS Foundation Trust to obtain signatories.
April 2012	Add Royal Cornwall Hospital Trust in Section 2 Add Peninsula Community Health in Section 2 and Appendix 3
Sept 2012	Remove Devon Primary Care Trust Up dated organisational titles
October 2012	Paragraph 1 – add wording for local information sharing to indentify risk and un-met needs Paragraph 2. Suggested new signatories and new para at 3rd bullet point in 4.5.to cover local information sharing meetings Add Appendix 6 – consent to share information form to assist frequent users of services
June 2014	Change title Replace CRB with DBS Paragraph 4.7. replace Vetting and Barring Service paragraph and replace with Disclosure and Barring Service paragraph. Paragraph 4.14 Replace Race Relations Act with Equality Act 2010
November 2014 – July 2015 Version 2	Add Practitioners Guide, FAQ's and flowchart. Add signatories – CCG's and new organisational titles Remove Peninsula Community Health and Probation Consultation with Devon and Cornwall Police Force Legal Dept re overall content Pressing need wording added in paragraph 5 Appendix 3 Add a FAQ re Serious Case Review and Root Cause Analysis Care Act 2014 references added Remove "vulnerable adults" and replace with "vulnerable persons" Paragraph 1 – Remove "vulnerable adults" replace with "adults with care and support needs/adults at risk". Insert bullet to detail definition of "vulnerable person". Paragraph 3 - Remove definition of "vulnerable adults" replace with "adults with care and support needs/adults at risk" definition. Paragraph 4.10 – Add paragraph on disposal of data. Paragraph 4.11 – Add paragraphs on breaches. Appendix 1 Add paragraph 8 – Should the adult at risk be at the Strategy meetings/case conference?

A APPENDIX 1 PRACTICTIONERS GUIDE FOR INFORMATION SHARING

PROPORTIONATE/RELEVANCE GUIDANCE

(to assist in determining what types of information might require further consideration)

Is the information proportionate/relevant?

Irrespective of classification of offence, does the information include any of the following elements/aspects;

- Abduction/kidnap/False Imprisonment/Hijacking
- Abuse of a position of trust involving children or vulnerable adults
- Action which could Endanger lives or cause harm
- Animal Cruelty
- Arson
- Child Protection matter
- Concealment of birth/death
- Domestic violence
- Drink/drug Driving & Dangerous driving-where relates to driving position and involves working with children or vulnerable adults
- Drug related
- Elder Abuse/Neglect
- Harrassement/intimidation/bullying/Blackmail/Bribery
- Human Trafficking
- Illegal medical practices
- Murder/manslaughter/genocide
- Perjury/Perverting the course of justice
- Racial Abuse/Religious Abuse/Hate crime
- Refusal/Revocation of firearms licence/Illegal firearms Possession/weapons
- Robbery
- Sexual/Pornography/Prostitution/Grooming
- Stalking
- Terrorism/Treason/War crime
- Theft/Burglary/Fraud-where related to contact with vulnerable adults
- Violence

YES

Relevant for further consideration

Could the information be categorised as:

- Argument-no violence
- Bigamy
- Breach of bail/absconding from custody
- Breach of the Peace
- Criminal Damage
- Driving offences not categorised in previous box
- Drunk & Disorderly
- Firearms license granted
- Liquor Licence offences
- Mental health status (no indication of risk)
- Military Admin offences (no crime)
- Non Payment of fines
- Piracy/Copyright
- Poaching
- Pollution-Noise/Environmental
- Routine check-nothing found
- Stop & Search-nothing found
- Theft/Burglary/Fraud-where related to contact with children
- Trespass
- Vagrancy

Yes

Not Relevant unless mitigating/aggravating factors

Proportionate/Relevance

Factual details regarding Cautions, Convictions, Warnings & Reprimands are normally disclosed if relevant.

Other information when considering information to disclose;

- How long ago did the incident occur?
- How old was the person at the time?
- Conduct of suspect now?
- Is the information trivial?
- Is the information evidence of risk?

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

Frequently asked questions

1. Does the Data Protection act 1998 prevent information sharing?

No. It is not a barrier to sharing information; it provides a framework to ensure that personal information is handled appropriately. Information sharing is essential to enable early intervention and preventative work, for safeguarding and promoting welfare and for wider public protection.

2. What do I do if I've gone through the flow chart and read this agreement and am still not sure?

Seek advice from your supervisor, manager or nominated person within your organisation or agency. If you are unsure of the information request, or it falls out of the safeguarding process as detailed on the flowchart, ask the requesting person to detail it and the justification for it on form VA1.

3. How much information should I share?

Only what is relevant and necessary. Do not assume you have to share the whole case file.

Under no circumstances will the police interview recordings of suspects/witnesses be released to another agency. Practitioners are able to give verbal accounts relating to recorded interviews of suspects/witnesses as part of the safeguarding process. If agencies require any further information relating to recorded interviews of suspects/witnesses this will be requested and recorded on form VA1. These disclosure requests will be authorised by the PPU unit Inspectors, who may wish to consult with the force Data Protection Manager/Force Legal department.

If requests for case documentation are made i.e. statements, the onus is on the requesting agency/organisation to seek the written consent of any witnesses for copies of police statements. Should the agency/organisation require witness details, these will be requested on form VA1 and be considered on a case by case basis.

4. Is all information confidential? If not when does Data Protection apply?

No, not all information is confidential. Confidential information is information of a private or sensitive nature that;

- Has been provided in circumstances where the person giving the information could reasonably expect it not to be shared with others.
- is personal information about an identifiable living person, or could enable a living person to be identified when considered with other information, it is personal information and is subject to data protection law. This is likely to be the case in most safeguarding work
- in order to protect the vital interests of the data subject or others

5. Do I need to seek consent?

Obtaining explicit consent in writing is best practice. Be open and honest from the outset with the person about why, what, how and with whom information will, or could be shared, and seek their agreement. You need to consider whether the person has capacity to understand and make their own decisions; if not it needs to be a 'best interest' decision (Mental Capacity Act 2005.) **You may still share information without consent if, in your judgement on the facts of the case, that lack of consent can be overridden in the following circumstances, to do so would;**

- Place an adult or child at increased risk of significant harm; or
- Prejudice the prevention, detection or prosecution of a serious crime; or
- Lead to an unjustified delay in making enquiries about allegations of significant harm or serious harm

6. Where do I record my information sharing decision?

If a form VA1 has been used then your decision and the reasons for sharing or not can be recorded on this. If you have shared information as part of the safeguarding process i.e. strategy meeting/ case conference your disclosure should be included on the minutes, which you will be expected to check for accuracy afterwards. If you have taken part in a strategy discussion then your disclosure and requests should be recorded on your agency's IT system relating to that person/case. Any discussions with managers relating to your disclosure should be recorded in the same manner as described. Requests for disclosure on form VA1 will be scanned and placed in an electronic file for the office/agency receiving requests i.e police requests will be dealt with by the officer in the case (OIC) and all requests and subsequent disclosures will be recorded on formVA1.It

is imperative that all the information on form VA1 is legible and scanned correctly.

7. Can I still share information at a safeguarding adult strategy/case conference with a non-statutory partner there?

Yes, however there should be discussion with the chair before the meeting commences as to what information is to be disclosed and possible implications of disclosure, which may affect how the meeting is run i.e. if a provider is going to be at strategy then police should be notified and discuss this beforehand. The strategy might be split into two; in the first part information is shared and discussed, reaching an agreement as to what can be shared with the provider in the second part.

In safeguarding adult meetings it is accepted that there may be other non-statutory agencies invited if appropriate i.e. Non council housing providers; the same discussions around the disclosure should take place with the chair. Information can be shared if appropriate under Data Protection-apprehension/prosecution of offenders, prevent/detect crime & to protect the vital interests of the individual, also Common Law-preserve & protect public safety.

8. Should the adult at risk be at the strategy meeting/case conference?

Yes, the Care Act stipulates that the adult should be involved and included from the earliest opportunity and their views and wishes should be sought prior to any meeting taking place. It should be assumed that the adult and/or their advocate will be present and therefore careful consideration should be given regarding the planning of the meeting and the information to be shared whether verbally or in written form. As Q7 above the strategy may be split into two where professionals can share sensitive personal information that the adult is not lawfully entitled such as suspect details, other witness details, other victim details and certain methods of obtaining evidence or police intelligence.

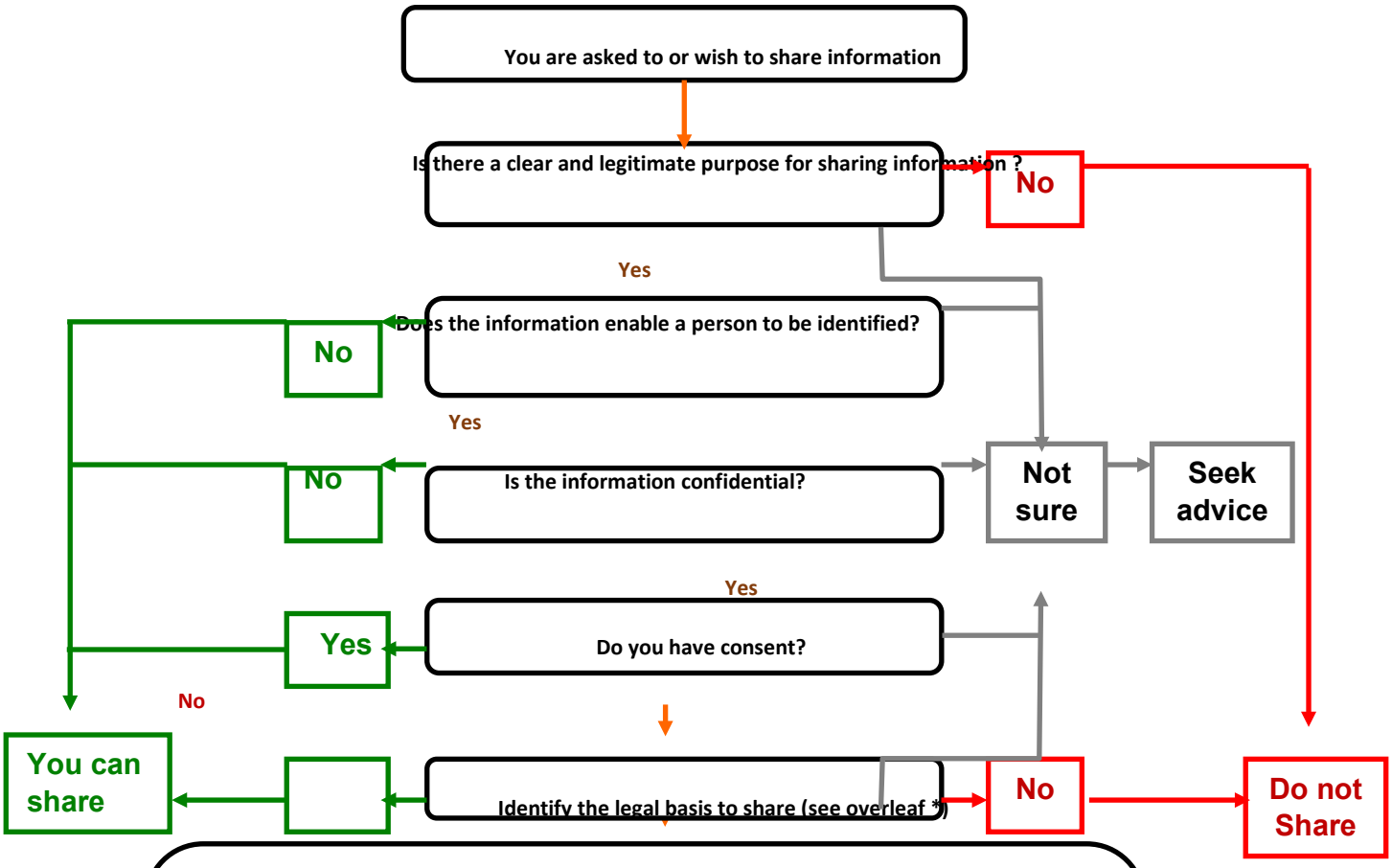
9. Can I disclose information for a Serious Case Review or a Root Cause Analysis Meeting?

In order to carry out its functions SABs will need access to information that a wide number of people or organisations may hold. Information requests for an SCR/SAR (which has been approved by the SAB) would normally be made through a SAB representative for your agency. Agencies may have dedicated resources for this function i.e all requests for police information should be forwarded to the Public Protection Unit, Serious Case Review Unit. For any other reviews i.e. single agency/SIRI's information protocols will be followed and a VA1 form completed unless it has been agreed & authorised by the SAB.

10. What if a partner organisation fails to share information about an individual that is relevant to safeguarding?

The Statutory guidance to the Care Act emphasises the need to share information about safeguarding concerns at an early stage and that local information sharing protocols should be in place & adhered to. If there is reluctance to share a VA1 form should be completed by the requesting agency detailing the request & lawful basis. The reasons for not sharing if applicable should be detailed fully. Continued reluctance to share by one agency should be referred to the SAB, who can then consider a request under clause 45 of the Care Act.

Flowchart of key questions for information sharing



Share Information:

- Identify how much information to share.
- Distinguish fact from opinion.
- Is it proportionate/relevant; see pages 15-18
- Requests for information falling outside of *safeguarding adult meetings (defined for this agreement as Strategy Meetings/discussions, Case Conferences) will need to be documented on form VA1 by person requesting
- Ensure that you are giving the right information to the right person.
- Ensure you are sharing the information securely.

Record the information sharing decision and your reasons in line with your agency's or local procedures.

If there are concerns that an adult is at risk of significant harm then follow the relevant procedures without delay

Seek advice if you are not sure what to do at any stage and ensure that the outcome of the discussion is recorded.

If you receive any complex requests for disclosure and/or your agency has completed its enquiries i.e. the police investigation has finished but another agency is continuing with disciplinary proceedings, the requesting agency must complete the disclosure form VA1

*Local information sharing meetings/professionals meetings requests for disclosure (these meetings ARE NOT part of the safeguarding adult process as defined in previous flow chart therefore information must be shared with consent or the lawful basis identified beforehand and documented. After initial disclosure appertaining to a data subject any subsequent disclosures (whereby consent has not been given or not appropriate) should be requested on form VA1. A separate form will be required for each data subject.

B APPENDIX 2 - PROCEDURES FOR INFORMATION REQUESTS AND DISCLOSURES

To demonstrate the legitimate exchange of data, where such an exchange takes place outside of the Safeguarding Adult process defined in this agreement as strategy discussions/meetings & Safeguarding Adult Case Conferences, request/disclosure documents are to be completed prior to disclosure wherever possible. Individuals completing request documents must ensure that the information requested is always limited to that which is necessary and/or expedient for the purposes of that enquiry.

The request form at Appendix 5 must identify the specific reason for the request for, or disclosure of, information.

The partners should respond to formal requests for personal data within two working days. However**,** there may be occasions when information is urgently needed. If it can be demonstrated that: -

- there is a real risk to the health of a data subject and/or
- it is needed to prevent serious injury to a data subject, staff or a member of the public

the information may be required to be disclosed within two hours of a request document being received. The nature of the requests and disclosures are such that normal mail systems cannot be used due to the time constraints. Communication will therefore always be via secure fax links direct to the office of the respective Nominated Officer or via secure email to a pnn.police, .gcsx.gov or nhs.net address. The sender of the information should be aware that some partners may use remote access to these emails via agency owned laptops or secure access via home computers. Partners deploying this type of remote access must ensure they comply with their responsibility to comply with Principle 7 of the Data Protection Act 1998 before implementing remote access, to ensure a level of security appropriate to;

a) the harm that might result from such unauthorised or unlawful processing or accidental loss, destruction or damage as are mentioned in the 7th principle and,
b) the nature of the data to be protected,

Upon receipt of an application, for disclosure, the receiving partner shall first establish whether any of the data requested was supplied to them by another partner.

If yes, the data owner shall be asked to confirm, in writing, that:

a) the data remains accurate, and
b) all the data may be disclosed.

If not, the recipient should disclose in accordance with their normal procedures. Referrals to other partners should not be delayed. Disclosures from those Signatories with Caldicott Guardians must be endorsed by the relevant Caldicott

Guardian unless the relevant Signatory notifies the Nominated Holder otherwise.

C APPENDIX 3 - LEGAL ISSUES

This agreement is focused on the sharing of information to protect vulnerable persons or adults with care & support needs/adults at risk. Within this process signatories can utilise the conditions within Schedule 2 and 3 of the Data Protection Act and the exemption within Section 29(3) to the Act to make disclosures without consent, where this is required to protect the vital interests of the data subject or others or where disclosure is necessary for the prevention or detection of crime.

Outside of this high-risk case scenerio, information provided by the data subject to the receiving agency would have been deemed to have been provided in confidence. and, where it is necessary to share personal data within the partners, any disclosure should be with the **informed, explicit, written consent of the data subject, or must be capable of being justified as an exception to the general Common Law Duty of Confidentiality and the Data Protection Act 1998.**

Data protection and confidentiality issues surrounding a disclosure will not apply if the consent of the individual has been sought and obtained. As this agreement deals with vulnerable persons/adults with care and support needs/adults at risk, where such persons are not able to write, the process that the subject person uses to identify themselves in their day to day interaction will be acceptable. Alternatively, where the subject person is unable to recognise the concept of informed consent, and thus cannot consent, a best interest decision (Mental Capacity Act (MCA) 2005) should be taken and recorded in accordance with the MCA Code of Practice, following the below provisions.

In the case of statements made to the police, informed consent must be sought in order to share statements supplied by individuals for their evidence to be used by other agencies. A tick box on the reverse of the MG11 is not deemed sufficient (see FAQ's page 17).

The partner's responsibility for service to its clients will at times clash with the responsibility of confidentiality to the individual. Risks to the safety of the individual person or adults with care & support needs/adults at risk – including members of the public and staff – requires prompt action and in such circumstances the presumption of confidentially can be set aside if there is a compelling reason of overriding public interest or there is a pressing need to disclose. Such a decision must be made only after taking into account the interests of all parties/subjects and all the circumstances of the case with as much information as can reasonably be obtained. Similarly such action can be taken, in the best interests of the data subject (i.e. where there is no public interest), under a Court Order or under a statutory obligation to disclose information. Prior to disclosure the nominated officer must consider, whether the personal information is held under a duty of confidence, and whether there is an overriding public interest or other justification for disclosing the information, thereby treating the disclosure of information as an exception to the general principals of confidentiality. This will apply even where the individual has refused to allow information to be shared.

Each disclosure must be treated on a case by case basis.

Details of witnesses or complainants, other than the alleged victims, must not be disclosed without their written consent.

Whilst disclosure with consent must be the overriding aim, where such consent is refused this will not necessarily act as a bar to the disclosure of information. Such disclosures can be made, subject to the legal powers conferred on some of the statutory agencies or the overriding issues of the prevention and detection of crime, safety or public interest. However, the remaining principles within the Data Protection Act 1998 must be adhered to by all parties to this agreement.

Legal Powers supporting Information Sharing within this agreement.

1. Information from the Police

1.1. **Data Protection Act 1998** – The conditions required by the Police to process the personal information linked to this agreement are;

Schedule 2: Conditions relevant for the First Principle; Processing of Personal Data.

1 With the consent of the data subject.

5(d) The processing is necessary for the exercise of any other functions of a public nature exercised in the public interest by any person.

6(1) The processing is necessary for the purposes of legitimate interests pursued by the data controller or by third party or parties to who the data are disclosed, except where processing is unwarranted in any particular case by reason of prejudice to rights and freedoms or legitimate interests of the data subject.

Schedule 3: Conditions Relevant for the First Principle; Processing of Sensitive Personal Data

1 With the explicit consent of the data subject.

3 The processing is necessary-

(a) in order to protect the vital interests of the data subject or another person, in a case where;

(i) consent cannot be given by or on behalf of the data subject, or

(ii) the data controller cannot be reasonably be expected to obtain the consent of the data subject, or

(b) in order to protect the vital interest of another person, in a case where consent by or on behalf of the data subject has been unreasonably withheld.

1.2. **The Code of Practice on the Management of Police Information**. - This code was developed under section 39 and 39a of the Police Act 1996 and enacted in November 2005. The code sets out principles governing the management of police information, including procedures governing authorised sharing of information obtained and recorded for policing purposes within the

police service, and with other agencies. A full Manual of Guidance on the Management of Police Information supporting the requirements of the code was published in March 2006 with a second edition in 2010.

Policing purposes are defined within the code as;

a) protecting life and property;

b) preserving order;

c) preventing the commission of offences;

d) bringing offenders to justice; and

e) any duty or responsibility of the police arising from common or statue law.

The code allows the police to disclose police information to other person or bodies where this is reasonable and lawful to do for the policing purposes as set out above. Any sharing of information must comply with the ACPO Guidance on the Management of Police Information 2006 and any agreement, national or local, which may be agreed with the persons or bodies needing to receive the information.

1.3. **The Crime and Disorder Act 1998** confers a power to share information, not an obligation, for the partners listed in Section 115 to do all they reasonably can to prevent crime and disorder. The partners listed as relevant authorities in Section 115 are the Police, Probation, Health and local authorities.

Disclosures can also relate to disrupting those who promote violent extremism and supporting vulnerable individuals in line with the HM Government strategy, where targeted and interventionist approaches will be co-ordinated within a Crime Reduction Partnership.

Disclosures cannot be made to the voluntary sector partners – or the non Council Housing Providers under the power of Section 115. However, within this agreement, disclosures without consent can be made by the statutory authorities under the following;

Common Law: where the public interest outweighs the presumption of confidentiality and where disclosure will preserve public safety and/or prevent or detect crime. In such circumstances regard must be given to the fact that such disclosure amounts to an exception to the general principle of confidentiality and in some cases, statutory obligations under the Data Protection legislation.

The Human Rights Act 1998 and European Convention of Human Rights: Article 8 of this convention provides the individual with a right of privacy. However, this does not preclude disclosures under this agreement which are made in accordance with the law, which are necessary in a democratic society and where they can be justified in the interest of public safety, to prevent crime and disorder and to protect the health, morals, rights and freedoms of others.

- Clause 45 of the Care Act focuses on the 'supply of information',and thus the SAB may request a person to supply information to it or another person ;

The person who receives the request **Must** provide the information provided to the SAB if;

- the request is made in order to enable or assist the SAB to do its job;
- the request is made of a person who is likely to have relevant information and then either ;
- the information requested relates to the person to whom the request is made and their functions or activities or;
- the information requested has already been supplied to another person subject to a SAB request for information.

The principles of information sharing should still be followed i.e. necessary, proportionate, relevant , accurate, timely & secure

2. Information from the National Health Service

2.1. The NHS has its own procedures governing the release of information to third parties, which are now being developed as part of the Caldicott arrangements. Each has appointed a senior professional as Caldicott Guardian to oversee confidentiality arrangements, including agreeing agreements for the sharing of any information with partner organisations. The Guardian is responsible for ensuring that any requests for information meet the confidentiality requirements of the NHS.

2.2. In addition, all health professionals, including the Caldicott Guardians themselves, owe a personal duty to ensure confidentiality and will be held accountable by the regulatory bodies such as the General Medical Council.

D APPENDIX 4 - INDIVIDUALS' RIGHTS OF ACCESS – POLICE PROCEDURES FOR HANDLING REQUESTS FOR ACCESS TO INFORMATION - (SUBJECT ACCESS)

The Subject Access provision of the Data Protection Act 1998 gives individuals the right to request a copy of the information held about them.

All requests for access to police held information should be forwarded to the Force Data Protection Officer at Force Headquarters.

- On receipt of a request, if the request refers only to information owned and processed by the police, the Force standard procedures should be followed.
- If personal data is identified as shared data, or belonging solely to another partner organisation, it will be the responsibility of the Force Data Protection Officer to contact the data owner. An example of this would be information that is held jointly with a Health organisation. The data owner should be contacted via the nominated contact person to determine whether they wish to claim an exemption to withhold the information under the provisions of the Data Protection Act.

  These provisions allow for situations where information is held:

- For the prevention or detection of crime,
- For the apprehension or prosecution of offenders
- For the assessment or collection of any tax or duty (Section 29 (1) of the 1998 Act)
- For certain types of information held for health, education and social work purposes, as specified by statutory instruments have just been published, and are available on the Internet at: http://www.homeoffice.gov.uk/ccpd/dpsis.htm
- That is relevant to the making of judicial appointments;
- In respect of a claim to legal professional privilege
- For preparing statistics or carrying out research;
- For backup purposes;
- Where disclosures are prohibited by law e.g. information contained in adoption records
- Where orders have been made modifying the right to subject access e.g. data held by financial regulatory bodies.

  Decisions for withholding information should be taken with care, and if necessary, professional advice sought. They should also be formally recorded in case of subsequent dispute. There is no requirement to inform the individual requesting access that information has been withheld from them for these purposes.

Third Party Information

Where you cannot comply with the request without disclosing information relating to another individual who can be identified from that information, you are not obliged to comply with the request unless: The other individual has consented (in writing) to the disclosure of the information to the individual making the request, or

- It is reasonable in all the circumstances to comply with the request without the consent of the other individual. In determining whether it is reasonable, regard shall be had, in particular to:
- Any duty of confidentiality owed to the other individual
- Any steps taken by the data owner with a view to seeking the consent of the other individual;
- Whether the other individual is capable of giving consent, and
- Any express refusal of consent by the other individual.

All correspondence and action taken should be recorded, and notes of meetings made where possible, in case of subsequent dispute from the individual that their request for information has not been adequately met.

<u>40 Day Time Limit</u>

Requests must be dealt with as quickly as possible, so that you can respond to the request within the 40 day statutory requirement from the date that sufficient information is received from the individual that enables you to process the request.

E APPENDIX 5: - VA1 FORM (INFORMATION ONLY AS SEPARATE TEMPLATE TO BE USED)

AGENCY REQUEST FOR INFORMATION IN RELATION TO SAFEGUARDING ADULTS

Person Requesting: Role

Tel No: _____ Agency: _____

Date & Time: _____

Signature: _____

1. Is the data subject a service user or perpetrator?
2. Have safeguarding adult procedures been instigated?
3. If yes; where is the process? i.e. strategy investigation case conference
4. Has police enquiry/investigation been finalised? If yes, When? OIC?
5. Have other information requests been submitted in relation to the enquiry? If yes give details.

Reason for submission of form please indicate Y/N;

i. Internal agency investigation Y/N iv) Local information sharing Y/N

ii. Complex request Y/N

iii) Review meeting Y/Niiv)Other ……...

Legal authority to share;

Please indicate the grounds below on which disclosure is sought

1. Has client consented? Yes/No
2. If No- would it thwart investigation to seek consent at this time or place adult at greater risk? (Give details)
3. Is disclosure necessary to prevent/detect crime/apprehend/prosecute offenders?(Data Protection Act) Yes/No (gIve details)
4. Is disclosure necessary to protect the vital interests of the client or other person?(Data Protection Act) Yes/No (give details)

Circumstances and information required:

(Please detail exact information required and state lawful basis to support request/s)

Reply:

Internal consultations (Names /Dates/Times/Decisions):

External consultations (Home Office/Information sharing Helpline)

We make this disclosure on the basis of the reasons identified in your request and agree to its use for this sole purpose. If any change or further use is sought, authorisation must be made by us, as the data controller. The information disclosed must be kept secure and accessed only by persons dealing with this enquiry. It should be noted that persons dealing with the enquiry may not have access to all information held on agency systems.

Person Completing: Print Name----------

Signature----------Date----------

Agency:_____Tel No:

F APPENDIX 6 - MODEL FORM FOR SEEKING INDIVIDUALS' CONSENT FOR DATA SHARING

CONSENT TO SHARE INFORMATION AGREEMENT

I understand that because of my frequent contacts with ……(insert agency), the public services in my area are concerned that I need help and assistance above and beyond what is currently provided to me. In order to achieve this, those public services need to share information about me in order to work together in my best interests.

What I can expect

I understand that in order to help me, those agencies working with me will:

- Work together to help me
- Share information that they have about me, where this is in my best interests

These agencies will be one or more of the following (please indicate which agencies)

Devon and Cornwall Police

Cornwall Council

Cornwall Partnership NHS Foundation Trust

NHS Kernow CCG

NHS England/ Devon Cornwall and Isles of Scilly Area Team

Council of the Isles of Scilly

Devon County Council

Devon Partnership NHS Trust

Northern, Eastern and Western Devon CCG

Northern Devon Healthcare NHS Trust

Plymouth Community Healthcare CIC

Plymouth City Council

Plymouth Hospitals NHS Trust

Royal Devon & Exeter Foundation NHS Trust

Royal Cornwall Hospitals NHS Trust

Torbay and Southern Devon Health and Care NHS Trust

Torbay Council

South Devon Healthcare Foundation Trust

South Devon and Torbay CCG

This agreement complies with the requirement for explicit consent to be given under Schedule 3 of the Data Protection Act 1998.

Service user's name:_____

Signed:_____Date_____

G APPENDIX 7 - NOMINATED OFFICERS FOR INFORMATION REQUESTS AND DISCLOSURES

Contact's Removed from the Website Copy