DEVON AND CORNWALL PARTNERSHIP INFORMATION EXCHANGE AGREEMENT FOR THE EXCHANGE OF OFFENDER INFORMATION FOR THE PURPOSE OF PREVENTION AND DETECTION OF CRIME AND THE IDENTIFICATION OF RE-OFFENDING

Devon & Cornwall Police
Building safer communities together

Making Communities Safer
Working Together

Version 1

Published September 2020

Contents

Appendices

Agreement for the Sharing of information under the Crime and Disorder Act 1998

1. INTRODUCTION (THE WHAT)

1.1. This agreement is to provide the framework for the exchange of personal data in accordance with the Crime and Disorder Act 1998, the Licensing Act 2003 and HM Government Prevent Strategy.

1.2. This agreement also provides a framework for the exchange of personal data in accordance with the Anti-Social Behaviour, Crime and Policing Act 2014. The Act is to make provision about anti-social behaviour, crime and disorder, including provision about recovery of possession of dwelling-houses; to make provision amending the Dangerous Dogs Act 1991, the Police Act 1997, Schedules 7 and 8 to the Terrorism Act 2000, the Extradition Act 2003 and Part 3 of the Police Reform and Social Responsibility Act 2011; to make provision about firearms, about sexual harm and violence and about forced marriage; to make provision about the police, the Independent Police Complaints Commission and the Serious Fraud Office; to make provision about invalid travel documents; to make provision about criminal justice and court fees; and for connected purposes.

At present, the requirements for the sharing of personal data remain the same as per the legal basis given in this Agreement.

2. PURPOSE (THE WHY)

2.1. The purpose of this agreement is to provide the framework for the exchange of personal data for relevant signatories with a statutory duty imposed on them by Section 17 of the Crime and Disorder Act 1998 to exercise their functions to do all that they reasonably can to prevent Crime and Disorder.

2.2. This agreement provides the basis for the exchange of personal data for relevant signatories with a statutory duty imposed on them by Section 185 of the Licensing Act 2003. To exercise their functions to do all that they reasonably can to ensure local people and visitors to Devon and Cornwall have a better opportunity to enjoy their leisure time safely without fear of violence, intimidation or disorder while, on or arriving or leaving licensed premises. The licensing objectives are:

- the prevention of Crime and Disorder
- public safety
- the prevention of public nuisance
- the protection of children from harm

2.3. This agreement also covers certain circumstances which include disrupting those who promote violent extremism and supporting vulnerable adults in line with the HM Government Prevent Strategy where intervention and support measures will be

determined and agreed by a multi-agency panel. This will very often be in line with existing partnership arrangements.

3. PARTNERS (WHO)

3.1. The following organisations, by receipt of the agreement holder of a signed certificate on page 12 are deemed to be partners to this agreement.

Devon and Cornwall Police
Cornwall County Council and Cornwall Fire and Rescue Service
Cornwall Partnership Foundation NHS Trust
Council of the Isles of Scilly
Devon County Council
Devon and Cornwall Probation Trust
Devon & Somerset Fire & Rescue Service
Devon Partnership NHS Trust
East Devon District Council
Exeter City Council
Livewell South West
Mid-Devon District Council
NHS Devon Clinical Commissioning Group (CCG)
NHS Kernow Clinical Commissioning Group
North Devon District Council
Northern Devon Healthcare NHS Trust
Plymouth City Council
Plymouth Hospitals NHS Trust
Royal Cornwall Hospitals NHS Trust
Royal Devon and Exeter NHS Foundation Trust
Teignbridge District Council
Torbay Council
Torbay and South Devon NHS Foundation Trust
Torridge District Council
West Devon Borough Council and South Hams District Council

3.2. The Signatories for the purposes of this Agreement are identified in Appendix 6. The Nominated Officers for requests and disclosures are identified in Appendix 7.

4. PROCESS (THE HOW)

4.1. This Agreement is primarily concerned with the exchange of Personal Data between the Signatories.

4.2. The Signatories agree that Disclosures of Personal Data shall not be made under this Agreement where a disclosure of De-personalised Data would, instead, suffice. For example, De-personalised Data consisting of aggregated data or statistical data may instead be disclosed.

4.3. In the event of a disclosure of De-personalised Data, including disclosures made under the Crime & Disorder (Prescribed Information) Regulations 2007, the Signatory receiving the request shall make the disclosure requested, subject to the following conditions:

4.4. The De-personalised Data shall only be used for the purpose for which it is requested and that that purpose shall accord with the Purpose;

4.5. The De-personalised Data shall not be Processed in such a way that information about a living individual may be extracted from the De-personalised Data. It is the responsibility of the disclosing party to ensure that de-personalised data cannot be re-personalised.

4.6. **REQUESTS FOR PERSONAL DATA**

All requests for Disclosures should be made by the Nominated Officer of the relevant Signatory and, for the avoidance of doubt, requests made by any other person from the relevant Signatory will be declined. There is a clear requirement that as part of this agreement all requests for disclosures must be appropriately authorised and documented.

4.7. All requests for Disclosures should be sent to the Nominated Officer of the relevant Signatory.

4.8. All requests for Disclosures must be made on the appropriate Form, a copy of which is attached at Appendix 2. The reverse of that Form contains references to reasons for Disclosures and the appropriate one is to be indicated to support each application for Disclosure.

In specific cases a partner who has a power of prosecution e.g. Trading Standards Dept, Benefit Fraud Offices, will make requests for information. In these cases and where there is a strong probability that the information to be supplied will be presented at a Criminal Court hearing, the requesting partner may ask for the information to be provided in formal statement format, e.g. Police Statement MG11 format. In these cases the disclosing officer could be called to any subsequent court hearing, to answer questions relating to the information provided.

4.9. Each completed Form submitted in support of a request for Disclosure should be delivered by Recorded Delivery post, in person or by secure email.

4.10. The preferred method for sending information is via secure email, although it is acceptable to use recorded delivery or delivery in person. Established email domains that will enforce encryption include email addresses to and from .gov.uk, .pnn.police.uk and nhs.net. Confirmation from the IT Security Officer or equivalent that encryption is enforced is required by the sharing partner if an alternative email domain is used. Secure email solutions can also be used if available (i.e. Egress). Emails should not be sent to personal email accounts (i.e. gmail, hotmail etc).

4.11. **Minimum Disclosure Necessary**

The Signatories agree that they will adhere to the principle that any Disclosure requested or made should be restricted to the minimum amount of Personal Data necessary to achieve the purpose of the Disclosure. This will be determined on a case by case basis.

4.12. **Proportionality**

The Signatories agree that if a Disclosure will in some way restrict the rights of the relevant Data Subject the relevant Signatory or Signatories (as may be appropriate) will consider the rule of proportionality. This is to ensure that a fair balance is achieved between the protection of the Data Subject's rights and the general interests of society.

4.13. **Making Disclosures in Response to Requests for Disclosures**

All Disclosures to a Signatory should only be made to the Nominated Officer of the relevant Signatory.

4.14. Disclosures from those Signatories with Caldicott Guardians must be endorsed by the relevant Caldicott Guardian unless the relevant Signatory notifies the Nominated Holder otherwise.

4.15. All Disclosures should be made using the appropriate Form, a copy of which is attached at Appendix 3.

4.16. The Signatories should respond to formal requests for Disclosure of Personal Data within ten working days of receipt of the request. However, it is acknowledged that there may be occasions when the Disclosure is required more urgently. In such circumstances, if it can be demonstrated that: -

- there is a real threat to the health of a Data Subject; and/or
- it is needed to prevent likely injury to a Data Subject;

The Disclosure may be made prior to a Form being submitted pursuant to paragraph 4.8. above. In such instances, and to maintain an adequate Disclosure trail, a retrospective request Form must be submitted within five (5) working days. In an emergency situation, faxed confirmation of a request may be made in accordance with paragraph 4.9 above.

4.17. Upon receipt of an application for Disclosure, the Signatory receiving the application shall first establish whether any of the Personal Data which is the subject of the

application was supplied to it by another Signatory. In the event that it was, the Signatory receiving the application shall, without delay, contact the Signatory from whom the Personal Data originated who shall, in turn, confirm in writing without delay that:

- the Personal Data remains accurate; and
- whether the Personal Data may be disclosed.

In the event that the Personal Data originated from the Signatory receiving the request for Disclosure, that Signatory should process the Disclosure in accordance with its normal procedures.

4.18. **Caldicott**

The Signatories also acknowledge that those Signatories in the health sector or which have Social Services Departments each have their own procedures governing the release of information to third parties, which have been developed as part of the Caldicott arrangements and that Signatories must comply with these. Those Signatories in the health sector or which have Social Services Departments shall notify the Nominated Holder of all and any such procedures with which they expect Signatories requesting a Disclosure to comply with and the Nominated Holder shall circulate details of the same to the Signatories.

Health and social care partners agree to access, share and disclose patient-identifiable information in accordance with the seven Caldicott principles:

1. Justify the purpose(s) of using confidential information.
2. Only use it when absolutely necessary.
3. Use the minimum that is required.
4. Access should be on a strict need-to-know basis.
5. Everyone must understand their responsibilities.
6. Understand and comply with the law.
7. The duty to share information can be as important as the duty to protect patient confidentiality.

Direct information exchange between an NHS Trusts / Foundation Trusts and the Devon & Cornwall Police will utilise the Information Sharing Agreement agreed between the police and Bevan Ashford in 2002, where the specific information request is linked to the three areas of this Agreement and the Trust is a signatory to this Agreement.

4.19. **Devon and Cornwall Police, under Crime and Disorder, where justified will disclose;**

Depersonalised data relating to crime or anti-social behaviour in the areas of housing owned or managed by the requesting signatory. Except where justified by a

request citing a specific requirement of disclosure to a greater level of detail, this information will be supplied to postcode level, providing there are at least five houses within the postcode. Such information will only be disclosed on the understanding that the user will not merge the supplied data with other data sets to develop Personal Data from this source.

Evidence relating to convictions for arrestable criminal offences providing the offence is not considered 'spent' under the Rehabilitation of Offenders Act 1974.

Evidence relating to cautions accepted for arrestable criminal offences within 12 months of the caution being given.

Evidence of Warnings Given under the Protection from Harassment Act 1997, where warnings are recorded by the police within a period of twelve months empowered by the Protection from Harassment Act 1997, and in line with Force Policy. This Policy requires that there should be at least two occasions on which harassment has taken place, supported by substantive evidence, before an official warning is issued

Evidence from police records of incidents of anti-social behaviour. This Disclosure is empowered by the Crime and Disorder Act 1998.

Copies of statements made to the police by third parties relating to evidence above, where written permission had been provided by the statement maker for the statements disclosure for use in civil proceedings.

Devon and Cornwall Police, under the Licensing Act, where justified will disclose;

All relevant convictions as defined in schedule 4 of the Licensing Act 2003, which are unspent under the Rehabilitation of Offenders Act 1974.

Disclosures relating to cautions for offences as detailed in schedule 4 of the Licensing Act 2003 will be made by Devon and Cornwall Police for a period of twelve (12) months after acceptance of the same.

Devon and Cornwall Police will allow Disclosure of warnings given pursuant to the Protection from Harassment Act 1997 in the event that two (2) or more warnings have been given in a period of twelve (12) months.

The Signatories understand that the exchange of personal data post conviction will be subject to a presumption of confidentiality but that this may be overridden on the grounds of public interest, as described in Appendix 1 Section 1.1 and 1.9.

4.20. **Restrictions on the Disclosure of Personal Data**

The Signatories acknowledge that details of victims, witnesses or complainants must not be disclosed without their written consent.

Disclosures relating to cautions will be made by the Devon and Cornwall Constabulary for a period of twelve (12) months after acceptance of the same.

Devon and Cornwall Constabulary will allow Disclosure of warnings given pursuant to the Protection from Harassment Act 1997 in the event that two (2) or more warnings have been given in a period of twelve (12) months.

The Signatories understand that the exchange of Personal Data post conviction will be subject to a presumption of confidentiality but that this may be overridden on the grounds of public interest, as described in Appendix 1 section 1.1 and 1.9.

4.21. **Under Crime and Disorder the Local Authorities, where justified, will disclose;**

Evidence, including complaints from neighbours or the public relating to criminal, immoral or anti social behaviour. This disclosure is empowered by the Crime and Disorder Act.

Under the Licensing Act the Local Authorities, where justified, will disclose;

Information which is held by or on behalf of the Authority for the purpose of the authority's powers and duties under the Licensing Act 2003.

4.22. **Disclosures at Meetings**

Signatories who anticipate making Disclosures at meetings should ensure they are empowered to do so and that such Disclosures are permitted by all relevant legislation prior to making any Disclosure.

Such Disclosures should be recorded within the minutes of the relevant meeting, these will be securely handled and only circulated to those who are entitled to receive the disclosure. The relevant Signatory or Signatories shall ensure that these minutes are securely retained for at least six (6) years.

It is suggested as a model of good practice, those Signatories making disclosures at meetings should clarify all issues reasonably relevant to any intended Disclosure, to include without limitation, confidentiality issues and powers to make the Disclosure, prior to the commencement of the relevant meeting.

Expressions of opinion should be clearly distinguished from factual information.

4.23. **Circulation, Retention and Destruction of Received Disclosures**

Signatories agree that all received disclosures will be securely handled and stored, and only circulated to those who are entitled to receive the disclosure, and that the person or organisation receiving the information has adequate safeguards and working practices in place to prevent the dissemination of disclosures to parties not entitled to receive them.

Signatories agree that all disclosed information will be retained for no longer than necessary, and only in relation to the purpose for which such information was disclosed, following which, all disclosed information will be securely disposed of or erased.

Devon and Cornwall Police may, at any time, audit disclosures that have been made to establish what information is still held and which has been securely disposed of or erased, and by which secure method disposal took place.

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:

1. The parties hereto are working in partnership in exercising their functions and their responsibility for the protection of the public.
2. This Agreement provides guidance on the exchange and use of personal data.
3. 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.
4. In respect of the indemnity the parties have agreed as follows:-

Provision of Information

(a) 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 (b) to (c) below.

(b) 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.

(c) 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.

(d) 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 to cover those costs and expenses identified in clause (a) 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.

(e) 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.

By signing below, the partners accept and will adopt the details standards statements included in this Agreement at Appendix 4 and the Indemnity, and agree to maintain the specified standards. In addition, the partners will not use, release or otherwise disclose any data whatsoever,

(a) For any other secondary use not specified under this Agreement or by regulations made there under; and/or

(b) To any organisation which is not a signatory to this Agreement.

6. CERTIFICATION – CRIME AND DISORDER AGREEMENT FOR THE EXCHANGE OF INFORMATION VERSION 1.0 - SEPTEMBER 2019

By signing below, the Signatories:

- accept and agree to be bound by the provisions contained in this Agreement;
- confirm their personal responsibility to inform all colleagues within their respective organisation that they too have read, understood and agreed to the terms of this Agreement.

It is recommended that Signatories retain a list of those colleagues who have read, understood and agree to the terms of this Agreement.

Signed on behalf of (Organisation)	
Signature	
Name	
Position/Role	
Date	

Appendices

A LEGAL ISSUES

A1. **Law Governing and Enabling the Exchange of Personal Data under this Agreement**

Legal Power to Make Disclosures

The Signatories recognise that they may each only make disclosures insofar as they are legally empowered to do so.

A.1.1. **General Data Protection Regulation and Data Protection Act 2018**

Sharing Personal Data with a Competent Authority or with a Public Authority for General Purposes.

A.1.1.1. **Part Three Processing to Part Two**

Reference Part 3, Chapter 2, 36 (4) - Personal data collected for any of the law enforcement purposes may not be processed for a purpose that is not a law enforcement purpose ***unless the processing is authorised by law***.

In the context of the police common law system, a broad approach is required and unless otherwise directed, may be interpreted along the lines of '**in accordance with national law**'. An explicit statutory provision need not apply, as long as the application of the law is clear and foreseeable. This means partners can include clear common law tasks, functions or powers, as well as those set out in statute or statutory guidance. Partners may also draw parallels to '**laid down by law**', in that the overall purpose, as at section 2 of this document, must be to perform a public interest task or exercise official authority, and that overall task or authority has a sufficiently clear basis in law

Special Category Data

If processing special category data from Part 3 into Part 2 then Signatories need to meet an additional condition for processing special category data under Article 9.

The Article 9 Processing Conditions are:

9(2)(a)	Explicit consent
9(2)(b) Schedule 1, Part 1	Employment
9(2)(c)	Vital interests
9(2)(d)	Not-for-profit PPRTU
9(2)(e)	Made public by the data subject
9(2)(f)	Legal claims, judicial capacity
9(2)(g) Schedule 1, Part 2	Substantial public interest (please refer to glossary) / rule of law
9(2)(h) Schedule 1, Part 1	Medical, Social Care
9(2)(i) Schedule 1, Part 1	Public health
9(2)(j) Schedule 1, Part 1	Archiving, Research and Statistics

A.1.1.2. **Part Three Processing to Part Two and Part Two Processing to Part Two**

This type of personal data sharing may occur between the Police and a Competent Authority or the Police and a Public Authority for a non-law enforcement purpose.

The data controller must comply with Principle one: fair, lawful and transparent.

Identifying the lawful basis for processing under GDPR Article 6.

There are 6 possible lawful bases for processing personal data under the GDPR Article 6:

- ***6(1) (a) Consent:*** *the individual has given clear consent for you to process their personal data for a specific purpose.*
- ***6(1) (b) Contract:*** *the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.*
- ***6(1) (c) Legal obligation:*** *the processing is necessary for you to comply with the law (not including contractual obligations).*
- ***6(1) (d) Vital interests:*** *the processing is necessary to protect someone's life.*
- ***6(1) (e) Public task:*** *the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.*
- ***6(1) (f) Legitimate interests:*** *the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests.* ***(Note: Legitimate Interest cannot apply where the Police are processing data to perform an official task.)***

It is recognised that no one lawful basis is seen as better, safer or more important than another, and there is no hierarchy in the order of the list in the GDPR.

It is accepted, however, that the sharing of personal data on a case-by-case basis for a **policing purpose** is likely to be shared in order to perform a **public task.**

Public Task – The Police can rely upon GDPR Article 6 (1) (e) as the lawful basis for processing personal data where the processing is necessary for the performance of a task carried out in the public interest and the task has a clear basis in law.

This includes the common law policing tasks and functions set out in MOPI 2005 (Policing Purpose) as well as those set out in statute (e.g. Crime and Disorder Act 1998) or statutory guidance.

Two examples:

The Police and the Local Authority are performing a task in the public interest and the power to share information is derived from:

- *The General Data Protection Regulation 2018 – Article 6(1)(e) – Public Task;*
- *Local Government (Miscellaneous Provisions) Act 1976 S51 – the Local Authority has an obligation to assess whether an individual is fit and proper to become a taxi driver; or*
- *The common law powers of disclosure.*

The 1976 Act provides a power to the Local Authority to process for these purposes, ***but there is no explicit gateway for disclosure into the purpose****.*

Any requests for disclosures will therefore be carried out on grounds of Common Law Police Disclosure, i.e. only where there is a pressing social need.

General Processing – Part 2 – Lawful Basis for Processing

GDPR 2018 Article 6 (1) – Legal Obligation. Partners can rely on legal obligation if they must process the personal data under statute. There is very little legislation that expressly requires the police to share personal data. Partners are encouraged to help the police identify any relevant legislation that expressly obliges the police to share information with them.

Criminal Conviction and Offence Data

If processing criminal conviction data or data about offences from part three to part two then compliance with GDPR Article 10 will apply.

Article 10 states: processing of personal data relating to criminal convictions and offences or related security measures based on Article 6(1) shall be carried out only under the control of official authority or when the processing is authorised by Union or Member State law providing for appropriate safeguards for the rights and freedoms of data subjects.

This means that where the police have identified a lawful basis for processing criminal offence data they must also ensure that they comply with the additional safeguards for the rights and freedoms of the data subjects.

Some of the other more common legal gateways / powers to share are contained in the following statutes or common law duties:

A.1.2. **Crime and Disorder Act 1998**

Under Section 17 the Relevant Authority has the duty to consider crime and disorder implications and the need to do all that it reasonably can to prevent:

- crime and disorder in its area (including anti-social and other behaviour adversely affecting the local environment);
- the misuse of drugs, alcohol and other substances in its area; and/or

- re-offending in its area.

Under Section 115(1) – Any person who would not have power to disclose information to a relevant authority or to a person acting on behalf of such an authority shall have power to do so in any case where the disclosure is necessary or expedient for the purposes of any provision of this Act.

A.1.3. **Licensing Act 2003**

Section 185 of the Licensing Act 2003 provides the power to exchange of information required in relation to the instituting of proceedings under the Act.

A.1.4. **Police Act 1996**

Section 39A – Chief Officers are required to give "due regard" to statutory code (Code of Practice on the Management of Police Information 2005).

A.1.5. **The Code of Practice on the Management of Police Information**

Reference 4.1 – Authorised Professional Practice on the Management of Police Information issued by the College of Policing ("APP") and the Code of Practice for Management of Police Information. This 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.

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. 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.

Additionally the Code of Practice sets out obligations on the persons or bodies receiving police information which equate to the requirements set out in this Agreement.

A.1.6. **The Policing Protocol Order 2011**

The Chief Constable is responsible for maintaining the Queen's peace and is accountable to the law for the exercising of police powers and to the Office of the Police and Crime Commissioner (OPCC) for delivering of efficient and effective policing, management of resourcing and expenditure by the police force.

A.1.7. **Consent**

Disclosures may be made if the consent of the Data Subject has been obtained or the Disclosure is made at the request of the Data Subject. Note that Data Subject consent is also subject to the Caldicott Principles outlined in Section 4.18 of this Agreement.

It is recognised by all partners that relying solely on consent as the lawful basis is difficult to manage and that it is inherently unfair to ask for consent where the police and/or partner(s) would process the personal data in any event to meet the policing duty or fulfil a public task.

For systematic and routine sharing, consent will be avoided where another lawful basis exist.

A.1.8. **Human Rights Act 1998**

Section 8(1) – All data subjects have a right to a private family which can only be interfered with if justified and proportionate.

Interference with this right may be justified where the processing is necessary and in the interest of:

- discharging the common law police duties
- preventing/detecting unlawful acts
- protecting public against dishonesty
- preventing fraud
- terrorist finance / money laundering
- safeguarding children and adults at risk, and/or
- safeguarding economic wellbeing of vulnerable adults

A.1.9. **Common Law Duty of Confidence**

In the case of personal data held under a duty of confidence a disclosure may be made in respect of that personal data if there is a compelling reason of overriding public interest or another overriding statutory justification which permits the disclosure.

The Signatories understand the public interest criteria to include (but not be limited to):

- the administration of justice
- maintaining public safety
- the apprehension of offenders
- the prevention of Crime and Disorder
- the detection of Crime, and/or
- the protection of vulnerable members of the community.

The signatories should confirm, check and verify the following points when deciding if the public interest criteria should override any duty of confidentiality:

- That the intended disclosure is proportionate to the intended aim?
- The vulnerability of those who are at risk where this is a factor to support the disclosure?
- The likely impact of the disclosure on the offender?
- That there is no other equally effective means of achieving the same aim?
- That the Disclosure is necessary to prevent or detect crime and uphold the rights and freedoms of the public?
- The disclosure of the information is necessary to protect other vulnerable people?

When considering or making any disclosure, the signatories should ensure they are compliant with Article 8 of the Human Rights Act 1998, which states that everyone has the right to respect for his private and family life, home and his correspondence, and that there shall be no interference by a public authority with this right except as in accordance with the law and is necessary in a democratic society in the interests of:

- national security
- public safety
- economic wellbeing of the country
- the prevention of crime and disorder
- the protection of health and morals, and/or
- the protection of the rights or freedoms of others

The signatories should confirm, check and verify relevant guidance issued by the Home Office and other Government Departments pursuant to or in respect of the Acts or laws referred to in this section from time to time provided that, in the event of any conflict between such guidance and the relevant Act(s) or laws then the Act(s) or laws (as may be appropriate) will prevail.

A2. **Partners Legal Powers to Share Personal Data with the Police**

A.2.1. **Conditions for Processing under the GDPR/DPA 2018**

Partners may share personal data with the Police provided that they have a **lawful basis** to do so and the purpose is **compatible** with the purpose for which the information was originally collected (principles one and two).

Disclosure from the general processing of one partner necessary to meet the **law enforcement purpose** of the other will occur by virtue of Article 6(1)(e); as referenced above.

Special category personal data strictly necessary to meet this purpose may be transferred under Article 9(2)(g) by virtue of Data Protection Act 2018:

Schedule 1 Part 2 (6) – statutory functions including common law provided in the substantial public interest.

- Schedule 1 Part 2 (10): preventing or detecting unlawful acts;
- Schedule 1 Part 2 (11) for protective functions (including regulation and vetting).
- Schedule 1 Part 2 (12) for regulatory functions.
- Schedule 1 Part 2 (18) for safeguarding functions.
- Schedule 1 Part 3 (30): Protecting individual's vital interests.

A.2.2. **Exemptions under the GDPR/DPA 2018**

Disclosure from the general processing of one partner necessary to meet the law enforcement purpose of the other may also occur by use of the exemptions as follows:

A.2.2.1. **Crime and Taxation: General**

DPA 2018 Schedule 2 Part 1(2) (a)(b)(c) dis-applies GDPR Article 15(1) to (3) to the extent that the application of those provisions would be likely to:

- prejudice the prevention or detection of crime;
- the apprehension or prosecution of offenders; or
- the assessment or collection of a tax or an imposition of a similar nature.

A.2.2.2. **National Security (DPA 2018 Section 26: National Security and Defence)**

(1) A provision of the applied GDPR or this Act mentioned in subsection (2) does not apply to personal data to which this chapter applies if exemption from the provision is required for:

(a) the purpose of safeguarding national security, or

(b) defence purposes.

A.2.2.3. **Identify the Compatible Purpose**

It is recognised that partners will ensure the appropriate record is kept when the new purpose of the processing is not incompatible with the purpose for which the personal data was originally collected.

For example, the partner carries out activity outside of the law enforcement purpose, but which assists the police to discharge the policing purposes of:

- protecting life and property
- preserving order
- preventing the commission of offences
- bringing offenders to justice, and/or
- any duty or responsibility of the police arising from common or statute law.

B REQUEST FORM FOR DISCLOSURE

REQUEST FOR DISCLOSURE OF PERSONAL DATA FORM

Headed paper of requesting Signatory – with name, address and contact information.
CONFIDENTIAL **Crime and Disorder Act 1998** **GDPR/Data Protection Act 2018** **ASB, Crime and Policing Act 2014** **Devon and Cornwall Partnership Agreement** **Request For Personal Data**
I am making specific enquiries for the purpose below and require personal information about:
Our Reference: Surname: All forenames: All previous surnames (if applicable): Also Known As/Alias: Place of Birth (if known) : Sex: M/F Date of Birth: Present Address: (with postcode) Previous Address: (with postcode)
The information I require is:

Purpose(s) For Which Information Is Required:- Provision of this information will have the assumed effect of success in the pursuance of:	**Tick**
Crime and Disorder Act – Anti Social Behaviour Injunction(s)	
Crime and Disorder Act – Sex Offender Order(s)	
Crime and Disorder Act – Parenting Order(s)	
Crime and Disorder Act – Child Safety Order(s)	
Crime and Disorder Act – Reparation Orders	
Crime and Disorder Act – Action Plan Orders	
Other Orders (please specify):-	
Licensing Act 2003	
HM Government Prevent Strategy	
Or Any Other Activity – please specify:-	
Failure to provide the information could jeopardise one or more of the following crime reduction objectives: (a) Crime prevention. (b) Crime detection. (c) Apprehension of offenders. (d) Prosecution of offenders. (e) Public safety. (f) Prevention of public nuisance. (g) Prevention of children from harm. Because:-	

I confirm that the personal data requested is required for the purpose indicated below and failure to provide the information will, in my view, be likely to directly prejudice that purpose.			
Signed:		Date	
Name (Capitals)		Rank/Job Title	

C DISCLOSURE FORM

DISCLOSURE OF PERSONAL DATA FORM

Headed paper of requesting Signatory – with name, address and contact information.

CONFIDENTIAL **Crime and Disorder Act 1998** *Devon and Cornwall Partnership Agreement for Crime and Disorder* **GDPR/Data Protection Act 2018** **Disclosure of Personal Data**			
To:		**Your Reference:**	
Further to your written request dated.....the information you have requested about: (Full Name)..... Address: …… is as follows:			
Signed		Date	
Name			
You are reminded that this information is supplied on the following basis: • the data must only be used for the specific purpose(s) for which it was requested; • the data must be retained securely and in accordance with the standards included in the Agreement; and • you will securely destroy the data when it ceases to be required for the specific purpose for which it was requested.			

D DETAILED STANDARDS

D1. **Nominated Officers**

Any change in a Nominated Officer will be notified to the Nominated Holder, in writing, by the relevant Signatory. The Nominated Holder shall then inform all other Signatories of the change made.

D2. **Accuracy of Data**

The Signatories acknowledge that they each have a responsibility to verify and maintain the accuracy of Personal Data held by them which is subject to this Agreement, this being a statutory duty set out in GDPR Article 5(1)(d) and DPA 2018 part 3, chapter 2, section 38.

Where an inaccuracy is discovered, after a Disclosure has been made, it will be the responsibility of the Signatory discovering the inaccuracy to bring this to the notice of the Signatory making the Disclosure, in writing, who will notify all other Signatories who have also received the same Personal Data from it of the inaccuracy and any correction required in respect of that inaccuracy.

In order to meet the obligations under this clause, Signatories are expected to record Disclosures made.

D3. **Data Standards**

The Signatories acknowledge that the national standard for making data (including Personal Data) "fit for use" is industry standard BS7666. The Signatories recognise the benefits which might be brought to the Disclosure process and other information sharing carried out under this Agreement by the Processing of data which they hold in accordance with this standard BS7666. To this end the Signatories will endeavour to adopt this standard in respect of such Processing to the extent that this accords with their respective internal policies and procedures in this regard.

D4. **Use of Personal Data and Confidentiality**

<u>Process in accordance with Purpose</u>

The Signatories shall only use and otherwise Process any Personal Data received by means of a Disclosure in accordance with the Purpose of this Agreement and any specific purpose identified on a Request for Disclosure Form submitted in accordance with the Process set out in Section 4.

<u>Confidentiality</u>

Each Signatory shall at all times keep confidential all Personal Data supplied pursuant to this Agreement.

<u>Publication of Personal Data</u>

Signatories may only publish Personal Data disclosed to them by another Signatory pursuant to this Agreement if such Personal Data is anonymised and presented in such a way that it is De-personalised Data.

Disclosure of Personal Data to another Signatory

For the avoidance of doubt, a Signatory which received Personal Data through a Disclosure made by another Signatory shall not disclose such Personal Data to a different Signatory without the consent of the Signatory which made the original Disclosure.

This clause shall survive termination of the Agreement or the withdrawal of or removal of any Signatory.

D5. **Security**

Each Signatory will take all reasonable steps to adequately protect the Personal Data received by it from another Signatory from both a technological and physical point of view from unauthorised or unlawful processing of the Personal Data and accidental loss or destruction of, or damage to, the Personal Data.

The Devon and Cornwall Police will grade the Personal Data provided to them, to restrict access, where this is applicable.

Without prejudice to this clause, each Signatory shall ensure that access to Personal Data and other information obtained from another Signatory pursuant to and/or in accordance with this Agreement by individuals employed or otherwise engaged by that Signatory shall be restricted to those individuals who require such access.

The Signatories recognise the merit of maintaining a full audit record of all disclosures made to them.

The Signatories acknowledge that the national standard for making data (including Personal Data) secure is industry standard ISO 27001 (formally known as ISO/IEC 27001:2005). The Signatories will endeavour to adopt this standard in respect of all Processing of Personal Data, De-Personalised Data and other data which they carry out as a result of this Agreement insofar as this accords with their respective internal policies and procedures in this regard. In respect of the secure storage of paper-based personal information at least one physical barrier should be in place to prevent unauthorised access unless otherwise stated. For the storage and removal of electronic personal information ISO 27001 should be adhered to.

The provisions of this clause will survive termination of the Agreement or the withdrawal of or removal of any Signatory.

D6. **Agents, Contractors and Service Partners**

Whereas the GDPR / Data Protection Act 2018 permits the sharing of Personal Data between Signatories to the Agreement it is recognised that the Signatories may wish and/or need to engage a third party Data Processor to Process all and/or any Personal

Data received through a Disclosure. When making a release of such Personal Data to a third-party Data Processor the relevant Signatory shall:

- ensure that an appropriate written contract is put in place between the Signatory and the Data Processor in compliance with GDPR Article 5(1)(f) and DPA 2018 part 3, chapter 2, section 40. The contract must make provision for and controls the Processing of personal data to be carried out by the Data Processor and confirmation that the Data Processor is to act only on the instructions of the relevant Signatory.
- obtain from the Data Processor sufficient guarantees in respect of the technical and organisational security measures governing the Processing to be carried out;
- ensure that it retains and/or obtains sufficient access rights to enable it to confirm that such guarantees are being complied with, to respond to any complaints and breaches made in respect of any Processing and to satisfy Subject Access Requests;
- take reasonable steps to ensure that the Data Processor complies with any such guarantees;
- take measures to ensure that the Data Processor does not transfer the Personal Data to a third party; and
- inform any other Signatory from whom it obtained any of the relevant Personal Data that the Processing is to be carried out by the Data Processor.

D7. **Retention and Disposal of Personal Data**

The Signatories acknowledge that GDPR Article 5(1) and DPA 2018 part 3, chapter 2, section 39, requires that excessive Personal Data must not be retained.

The Signatories agree that they must destroy Personal Data provided to them under this Agreement as soon as it is no longer required for the original purpose for which it was supplied or collected.

In order to meet their obligations under this Section, all Signatories are expected to introduce a procedure and nominate a person to conduct reviews of Personal Data received through a Disclosure on a regular basis and at least every six months.

D8. **Subject Access Requests and Other Rights of Data Subjects**

The Signatories acknowledge that Data Subjects have, amongst other rights, a right to access certain Personal Data relating to them held by or under the control of Data Controllers pursuant to GDPR Article 15 and DPA 2018 part 3, chapter 3, section 45.

The Signatories agree that they shall apply their own internal procedures to deal with Subject Access Requests made in respect of access to Personal Data held by them. Where the Subject Access Request relates in whole or in part to Personal Data received from other Signatories through a Disclosure, the Signatory on receipt

of the Subject Access Request shall also apply the Subject Access Request Procedure set out in Appendix 8.

The Signatories shall each comply with their own internal procedures when dealing with notices received from Data Subjects which are made under the GDPR/DPA Act 2018 in respect of Personal Data held by them. Where the notice relates in whole or in part to Personal Data received from other Signatories through a Disclosure, the Signatory on receipt of the notice shall, where reasonably appropriate, consult with the Signatories who made the Disclosures.

The Signatories shall each comply with the provisions of the GDPR/DPA 2018 when handling Subject Access Requests and any other notices received from Data Subjects which are made under the GDPR/Data Protection Act 2018.

The Signatories recognise that the GDPR/Data Protection Act 2018 does not cover data relating to deceased persons and that, accordingly, requests received from third parties for access to data relating to deceased persons will not be treated in the same manner as Subject Access Requests. The Signatories recognise that access to such data is covered by the Access to Health Records Act 1990 (as amended) and the common law of confidentiality. The Signatories agree that request for access to such data will be dealt with in accordance with their own respective internal procedures with consultation with other Signatories where reasonably appropriate in the event that any of the data concerned originated from such other Signatories by means of a Disclosure.

D9. **Complaints**

Any and all complaints made in respect of Disclosures or other matters relating to this Agreement or addressed in this Agreement will be brought to the attention of the Nominated Officer of the relevant Signatories by the Signatory receiving the complaint, and they will be dealt with in accordance with the relevant internal policies and procedures of the relevant Signatories.

Signatories will keep each other informed of developments following a complaint received, where relevant.

D10. **Compliance and Good Practice**

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

D11. **Regular review of agreement and consultation regarding agreement**

The Nominated Holder shall ensure that a review of the Agreement is carried out by the Signatories:

- within the first six months of the date of the Agreement being signed;
- on an annual basis; and

- in the event that any new legislation comes into force or official guidance is issued which impacts on the Agreement or the obligations of all or any of the Signatories under the Agreement.

The Signatories shall consult with each other regarding matters of policy and strategy which directly arise from or in any way impact on this Agreement.

D12. **Changes to the Agreement**

All and any signatories may request any change to the Agreement at any time by submitting a request to the Nominated Holder.

Upon receipt of any requests for changes to the Agreement the Nominated Holder shall:

- circulate the requests to all the Signatories;
- co-ordinate responses received from any Signatories to the same; and
- where appropriate, seek the agreement to the requested changes from the Signatories.

No change shall be made to the Agreement except with the agreement of all of the Signatories, which agreement shall be recorded in writing.

A memorandum of any changes to this Agreement agreed by the Signatories from time to time shall be endorsed upon this Agreement and the Nominated Holder shall be responsible for arranging the same.

D13. **Changes to Signatories**

Withdrawal/Removal of Signatory from Agreement

Any Signatory may withdraw from being a Signatory to this Agreement upon giving written notice to the other Signatories.

In the event that a Signatory materially breaches a term of this Agreement or persistently breaches the terms of this Agreement, the other Signatories may upon a majority vote where each Signatory other than the Signatory in breach has one vote, remove that Signatory's status as a Signatory of this Agreement provided that all of the other Signatories submit their vote.

The Signatories will do all acts and enter into all such documents as are necessary to give legal effect to the withdrawal or removal of a Signatory pursuant to this section.

All Personal Data received by means of Disclosures from other Signatories must be returned or destroyed at the reasonable request of those Signatories in the event of a Signatory withdrawing from or being removed from this Agreement.

Any Signatory who withdraws or is removed from this Agreement must continue to comply with the terms of this Agreement in respect of any information (including Personal Data) that the Signatory has received as a result of being a Signatory to this Agreement.

D14. **Additional Signatories**

Third parties may also become Signatories to the Agreement where this is necessary or expedient to the successful implementation of the Purpose or necessary expedient to that third party's compliance with any statutory duty imposed on it.

The Signatories shall do all acts and enter into all such documents as are reasonably necessary to give legal effect to a third party, becoming a party to this Agreement where appropriate.

D15. **Registration/Notification under the DPA 2018**

Each Signatory will ensure that it holds a current notification with the Office of the Information Commissioner under the DPA 2018 at all times to receive, disclose and otherwise Process Personal Data in accordance with the provisions of this Agreement.

D16. **Compliance with GDPR/DPA 2018**

Each of the Signatories shall ensure that it complies with the GDPR/DPA 2018 at all times in respect of its Processing of Personal Data which is the subject of this Agreement.

Each Signatory shall ensure that it complies with the first data protection principle when obtaining and otherwise processing Personal Data which is the subject of this Agreement, unless for any reason stated in GDPR/DPA 2018 or other relevant legislation such compliance is not required or only partial compliance is required.

D17. **Freedom of information Act 2000 - Publication of Agreement**

This Agreement is accepted as a document for disclosure in line with the public authority partner's duties under the Freedom of Information Act 2000 and can be included in its Publication Scheme.

D18. **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.

D19. **Third Party Rights**

A person who is not a Signatory to this Agreement has no right under the Contracts (Rights of Third Parties) Act 1999 to enforce any term of this Agreement.

D20. **Counterparts**

This Agreement may be entered into in any number of counterparts and by the signatories to it in separate counterparts, each of which when so executed and delivered shall be an original.

E DEFINITIONS

PART I: GLOSSARY

In this Agreement the following words shall have the following meaning unless the context otherwise requires:

"Ancillary Agreements"	means all and any information Agreements entered into pursuant to paragraph 2;
"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"	means 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;
"Competent Authority"	1) In this Part, "competent authority" means— (a) a person specified or described in Schedule 7, and (b) any other person if and to the extent that the person has statutory functions for any of the law enforcement purposes (reference DPA Part 3, Chapter 1 (30))
"Controller"	means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law. (reference GDPR Article 4(7) and DPA Part 3, Chapter 1 (32)(1);
"Processor"	means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller (reference GDPR Article 4(8) DPA Part 3, Chapter 1 (32)(3)).;
"Data Subject Access Right"	Data subject is entitled to obtain from the controller; (a) confirmation as to whether or not personal data concerning him or her is being processed, and

(b) where that is the case, access to the personal data and the information set out in subsection (2).

Reference GDPR Article 15, 20 and DPA Section 45, Part 7 (185)(4).

"Data Subject" and Identifiable Person"	means one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person (reference GDPR Article 4(1)).;
"De-personalised Data"	means any information where any reference to or means of identifying a living individual has been removed;
"Disclosure"	means a disclosure by one Signatory to any other Signatory of Personal Data;
"Disorder"	means a level or pattern of Anti-social Behaviour within a particular area;
"DPA 2018"	means the Data Protection Act 2018;
"Nominated Holder"	means the nominated holder of this Agreement, which shall be the Data Protection Officer of Devon and Cornwall Police;
"Nominated Officers"	means all those individuals identified in Appendix 7
"Personal Data"	means any information relating to an identified or identifiable national person ('data subject'), who can be identified from those data, or from those data and other information which are in the possession of or are likely to come into the possession of any Signatory. They include, without limitation, any expression of opinion or intentions in respect of such a living individual. Reference GDPR Article 4(1).
"Personal Data Breach"	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed (reference GDPR Article 4(12) and DPA Part 3, Chapter 1 (33)(3).
"Processing"	Any operation or set of operations which is performed on personal data or on sets of personal

	data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction (reference GDPR Article 4(2)).
"Agreement"	means this Agreement;
"Purpose"	means the purpose of this Agreement, as set out in paragraph 2;
"Relevant Authority"	means any of those bodies or persons described in section 115(2) of the Crime and Disorder Act 1998 and "Relevant Authorities" shall be interpreted accordingly;
"Special categories of Personal Data"	means the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation (reference GDPR Article 9(1))
"Signatories"	means the signatories/partners to this Agreement which are identified in Section 3 and, for the avoidance of doubt, "Signatory" shall mean any one of them;
"Substantial Public Interest"	In reference to Appendix 1 - 1.1.1 Substantial Public Interest could include functions or tasks relating to: • Statutory, common law, government • Administration of justice, parliamentary functions • Equality or opportunity of treatment • Racial/Ethnic diversity at senior levels • Preventing/detecting unlawful acts • Protecting public against dishonesty, etc. • Regulatory activity re: unlawful acts, dishonesty • Journalism (PI, intent to publish) • Preventing fraud (anti-fraud orgs) • Terrorist finance / money laundering • Disability / MH support organisations • Counselling • Safeguarding children and adults at risk

- Safeguarding economic wellbeing of vulnerable adults
- Insurance
- Occupational pensions
- Political parties (political opinion)
- Elected representatives (requests to)
- Disclosures to elected representatives
- Elected representatives (prisoner data)
- Publication of legal judgements
- Anti-doping in sport
- Integrity of sports and sporting events

"Third Party"	means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data (reference GDPR Article 4(10)).
"Working practice agreements ancillary to this Agreement"	means specialised working practices agreed with specific partners which use the Crime and Disorder Act 1998 as the main power for disclosure, and directly link to the aims of this Agreement e.g. disclosure of police images to council CCTV units.

PART II: INTERPRETATION

1. In this Agreement where the context requires:

   i. the masculine gender includes the feminine and the neuter and the singular includes the plural and vice versa;

   ii. references to any statute or statutory provision include a reference to that statute or statutory provision as from time to time amended, extended or re-enacted and also include any subordinate legislation made thereunder from time to time;

   iii. references to clauses and appendices are, unless otherwise stated, references to clauses in and Appendices to this Agreement.

2. In this Agreement headings are for ease of reference and shall not affect it interpretation.

F SIGNATORY CONTACT INFORMATION PARTNERSHIP CONTACT OFFICERS

Signatory contact information has been removed from the external website version of this Agreement.

G NOMINATED PERSONNEL FOR INFORMATION REQUESTS AND DISCLOSURES

Signatory contact information has been removed from the external website version of this Agreement.

H PROCEDURES FOR HANDLING SUBJECT ACCESS REQUESTS

1. All Signatories should have internal procedures in place for handling and responding to Subject Access Requests (i.e. requests for access to Personal Data made pursuant to GDPR Article 15 and DPA 2018 part 3, chapter 3, section 45.

2. The following procedures should also be used for dealing with Subject Access Requests in respect of Personal Data which is held for Crime and Disorder purposes:

- On receipt of a Subject Access Request, if the request refers only to Personal Data Processed by the Signatory receiving the request, that Signatory should follow its own standard procedures for dealing with such requests.
- On receipt of a Subject Access Request, if the request refers to any Personal Data which originated from another Signatory it will be the responsibility of the Signatory receiving the Subject Access Request to contact the Signatory from whom the Personal Data Originated via the nominated contact person to determine whether they wish to claim an exemption to withhold the Personal Data under the provisions of GDPR or DPA 2018.
- Any decisions made to withhold Personal Data from a Data Subject should be taken with care, and if necessary, legal or other appropriate professional advice sought. They should also be formally recorded in case of subsequent dispute. There is no requirement to inform the Data Subject requesting access that Personal Data has been withheld from them for these purposes.

3. **Third Party Information**

3.1. When a Signatory cannot comply with a Subject Access Request without disclosing information relating to another **individual** who can be identified from that information, the provisions of GDPR Article 15 or Chapter 3 (Rights of the Data Subject) sections 43 to 45 of the Data Protection Act 2018 shall govern whether or not the disclosure is made to Data Subject making the Subject Access Request.

4. **Time Limit for Dealing with Subject Access Requests**

4.1. Subject Access Requests must be dealt with as quickly as possible in order to ensure that responses to Subject Access Requests are within the 30 day period required by statute. The 30 day period commences from the date that sufficient information is received from the Data Subject that enables the Signatory to process the Subject Access Request.

I REVISION INFORMATION

Previous Revision history for Version 1 and 2 of this Agreement has been retained and is available on request.

Version 1	September 2019	