SAFER CORNWALL

Kernow Salwa

COMMUNITY SAFETY INFORMATION SHARING PROTOCOL

Devon & Cornwall POLICE

CORNWALL FIRE & RESCUE SERVICE
A service of Cornwall Council

Probation Service

NHS
Cornwall and Isles of Scilly

one and all · owen hag oll
CORNWALL COUNCIL

Version history				
Date	**Version**	**Author/Editor**	**Comments**	**Approved by**
16/10/23	1.0	Erika Sorensen, Amethyst Community Safety Intelligence Team erika.sorensen@cornwall.gov.uk	None	Simon Mould (Safer Cornwall Chair) simon.mould@cornwall.gov.uk

Document Owner

This Information Sharing Protocol is owned by the Strategic Board of the Safer Cornwall Partnership.

The Amethyst Community Safety Intelligence Team acts as the single point of contact for any queries on its content.

Commencement & Review

The commencement date of this Protocol will be **1 November 2023**. This Protocol will be reviewed annually or sooner if relevant developments or issues dictate.

Contents

Background and Purpose

Background

The Crime and Disorder Act 1998 (and subsequent amendments)[1] sets out the statutory requirements for **responsible authorities to work together** with other local agencies, organisations, and people, to develop and deliver strategies to tackle crime and disorder and help create safer communities. These **statutory partnerships** are known as Community Safety Partnerships (CSP).

In January 2023 the Police, Crime, Sentencing and Courts Act introduced a new duty on specified authorities to collaborate and plan explicitly to **reduce and prevent serious violence**. Local areas are encouraged to adopt a **public health approach** and sharing information is a critical component.

Safer Cornwall has been agreed as the **lead partnership for the Serious Violence Duty**.

The following organisations are thus named as responsible/specified Authorities within the Safer Cornwall Partnership:

- Devon and Cornwall Police
- Cornwall Council
- Cornwall Fire & Rescue Service
- Cornwall and Isles of Scilly Youth Justice Service
- NHS Cornwall and Isles of Scilly Integrated Care Board
- Probation Service

The purpose of sharing information[2] within the Safer Cornwall Partnership is to:

- Develop intelligence in the form of **intelligence products** (such as strategic assessments, problem profiles and tactical assessments) and to identify new incidents and emerging issues
- Support the **delivery of services** to particular groups or individual people
- Support **performance and outcomes** monitoring

The **Partnership is responsible for putting in place a protocol** to facilitate information sharing between Safer Cornwall member organisations in Cornwall. All organisations play a role in supporting the sharing of information between and within organisations and address any barriers to information sharing to ensure that a **culture of appropriate information sharing** is developed and supported.

Whilst the term 'Partnership' is applied to all those who sit round the table, legally, only the responsible authorities have a statutory duty to meet these requirements.

The protocol reflects the **General Data Protection Regulation** ("UK GDPR") and **Data Protection Act 2018**.

The Partnership's Terms of Reference is published on the Safer Cornwall website.

[1] Police Reform Act 2002, Clean Neighbourhoods & Environment Act 2005 and Police & Justice Act 2006
[2] For the purposes of this protocol the term "information" will be used to include "data", as defined in the Data Protection Act and "information " as defined in the Crime and Disorder Act and Police and Justice Act

Purpose

The purpose of this protocol is to **facilitate the lawful exchange of information** to support **effective partnership working** and compliance with the statutory duties placed on Community Safety Partnerships.

This Information Sharing Protocol specifically seeks to:

- **Govern the use and management of information** by the Safer Cornwall Partnership for the purposes of developing and implementing **partnership plans, strategies and tactics** to prevent and reduce crime and disorder, including anti-social and other behaviour adversely affecting the environment, reoffending by adults and young people, serious violence and the problem use of drugs and alcohol.
- **Facilitate secure exchange** of depersonalised information between signatory agencies.
- Set out a framework for partner organisations and their staff to **process, share personal and special category data** on a lawful, fair and transparent basis with the purpose of enabling them to meet both their statutory obligations and the needs and expectations of the people they serve.
- Set out the principles that underpin the **secure and confidential sharing of information** between organisations involved in delivering services to people living and working within Cornwall, including a template for creating **Information Sharing Agreements** (Appendix 5) for multi-agency meetings where sharing of personal data occurs.
- Enable partnership involvement in the police intelligence structures through the secure sharing of **Strategic Threat and Risk Assessments** and other intelligence products to support partnership engagement at a local level in tackling serious and organised crime.[3]
- Enable statutory authorities to more effectively **meet their obligations under Section 17** of the 1998 Crime and Disorder Act and the amendments made by the Police and Justice Act 2006.
- Ensure that the **exchange of information**, including by electronic means, is undertaken **securely and safely**.
- Provide guidance on the **storage, retrieval and disposal** of information.

This Protocol applies to chief officers, elected members, executive directors, non-executive directors, trustees and all employees including volunteers and agency staff of the organisation and partner organisations who are signatories.

The Protocol also applies to **any organisation or agency, commissioned to deliver services** on behalf of any organisation party to this Protocol subject to granted permission to the third party organisation to disclose information by consent of the Controller.

The Protocol is intended to **complement any existing professional Codes of Practice** that apply to any relevant profession working within any organisation including the UK General Data Protection Regulation (UK GDPR) and Data Protection Act 2018 (DPA), but does not cover an individual organisations compliance to the UK GDPR or DPA and does not constitute legal advice. See Appendix 2 for a non-

[3] For example, '5C4P' Plans, tactical MoRiLE workshops and Clear, Hold and Build plans

exhaustive **list of relevant legislation** that may affect the ability to share information.

Partners should consider the likely effect of not sharing information, for example, harm to individuals, damage to their organisations' reputation, disconnect in partnership working and lack of understanding of issues.

This ISP **may not supersede existing information sharing protocols**, although partner agencies have agreed to operate under this ISP wherever possible.

This protocol sits beneath the overarching **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) which is owned by Devon and Cornwall Police and was last reviewed in 2020.

Information exchange for **the following multi-agency arrangements are excluded** from this Protocol:

- Multi-Agency Public Protection Arrangements (MAPPA)
- Domestic Abuse and Sexual Violence (including Multi-Agency Risk Assessment Conferences (MARAC))
- Prevent and Channel
- General safeguarding principles under Local Safeguarding Children and Safeguarding Adults arrangements.

Who will be sharing information?

Responsible authorities

Partners who are required to share information are the responsible/specified authorities in the Crime and Disorder Act 1998, as amended in the Police and Justice Act 2006, the Policing and Crime Act 2009 and most recently, the Police, Crime, Sentencing and Courts Act 2022.

The following organisations are named as responsible/specified authorities within the Safer Cornwall Partnership:

- Devon and Cornwall Police
- Cornwall Council
- Cornwall Fire & Rescue Service
- Cornwall and Isles of Scilly Youth Justice Service
- NHS Cornwall and Isles of Scilly Integrated Care Board
- Probation Service

Co-operating bodies

Co-operating bodies are important in **supporting the development of strategic assessments** and the **implementation of partnership plans**.

Co-operating bodies under the Crime and Disorder Act[4] may be asked to share information. These are the **Town and Parish Councils**, School and College **Governing bodies** and **Registered Social Landlords**.

From 31 January 2023, under the Serious Violence Duty, **educational institutions and prisons/youth custodial establishments** are required to collaborate with specified authorities if requested. They can also request to be involved themselves. The specified authorities must consult with all such institutions in their area in the development of a local strategic needs assessment and response strategy for serious violence.

Relevant Authorities for the purposes of Section 115

The effect of Section 115 of the Crime and Disorder Act 1998 is to allow **disclosure of personal data** to a "relevant authority" if it is **necessary or expedient** for the purposes of any provision of the Act. Relevant authorities are defined as:

- Police forces
- Local authorities
- The Probation Service
- Fire and rescue authorities
- Integrated Care Boards
- A person registered under Section 1 of the Housing Act 1996 as a social landlord (by virtue of Section 219 of the Housing Act 2004)

Other partners

The **Safer Cornwall Strategic Board approves this protocol**. **All member organisations** of this Board sign up to the principles of the protocol by virtue of their membership (listed below) and are able to share personal and depersonalised data for CSP activity.

- Cornwall Council
- Cornwall Fire & Rescue Service (part of Cornwall Council)
- Devon and Cornwall Police
- NHS Cornwall and Isles of Scilly Integrated Care Board
- Probation Service
- Cornwall and Isles of Scilly Youth Justice Service (part of Cornwall Council)
- Office of the Police and Crime Commissioner for Devon, Cornwall and Isles of Scilly
- South Western Ambulance Service NHS Foundation Trust
- Department for Work and Pensions
- Office for Health Improvement & Disparities
- Cornwall Association of Local Councils
- Voluntary Sector Forum
- Safer Stronger Communities
- Safer Scilly
- Our Safeguarding Children Partnership
- Cornwall and Isles of Scilly Safeguarding Adults Board

[4] Section 5(2)(c) of the Crime and Disorder Act provides details of persons or bodies required to co-operate with the Responsible Authorities in their exercise of the functions conferred by section 6 of that Act.

Various other bodies as invited participants under the Crime and Disorder Act may be asked to share data for crime and disorder purposes. Wider partners may also be required to share information in specific circumstances. These could include schools, other health agencies and voluntary sector organisations.

Other partners can formally sign up to the protocol. Where an **agency has not signed up** to the protocol, but a **partner/partners wish to share personal data** with them, **extra care** is required to ensure they understand the sharing and handling of sensitive information they see. It may be necessary to provide specific instructions and handling arrangements and ensure the agency representatives sign a **confidentiality declaration** to confirm that they understand their responsibilities. See Appendix 6 for a sample confidentiality declaration.

Responsibilities of signatories

The Protocol should be **signed by the Chief Officer or the Caldicott Guardian** for each organisation. Signatories to this Protocol are committed to the implementation of an appropriate level of Information Governance throughout their organisation, in accordance with recognised national standards.

To achieve these principles, Partner organisations agree to:

- **Adhere to the principles and commitments of this Protocol** whenever exchanging personal information, whether with a co-signatory or other agency/organisation.
- **Share statistical and anonymised/pseudonymised data wherever possible**, eliminating the use of personal information except where reasonably necessary.
- Ensure that **all staff are aware of and comply with their responsibilities** arising from both the Protocol and relevant legislation, and receive adequate training in order to do so. This includes temporary employees, contractors and volunteers.
- **Implement their own policies** on confidentiality, data protection, information security, records management and information quality, which are appropriate to their organisation and comply with recognised codes of practice.

Signatories to this Protocol will also establish efficient and effective procedures for:

- **Obtaining, informed consent** to collect, share and process personal information wherever reasonably practicable and where appropriate.
- **Informing individuals** what information is collected and shared about them.
- Addressing **complaints arising from the misuse or inappropriate disclosure** of personal information arising from information sharing decisions.
- **Enabling access to records of individuals** by those individuals on request.
- **Amending inaccurate records** and informing partners where these are shared.
- Review and destroy information in accordance with **good record management** practice and organisational policy.

- **Sharing information without consent when necessary**, recording the reasons for that disclosure (including legal basis) and the person responsible for making the decision
- **Making information sharing an obligation on staff** and allocating senior staff responsibility for making complex disclosure decisions.
- **Protecting personal information at all times**, with appropriate protective marking, security and handling measures and in accordance with the Government Security Classification Scheme (see Appendix 3 for how these translate to Cornwall Council's Classification Scheme).
- Developing and working to **detailed, specific information sharing agreements** that support identified purposes.
- Ensuring that **future developments in technology** reflect the requirements of the UK GDPR, DPA 2018 and this Protocol and any that any information sharing is secure and can comply with the UK GDPR and DPA.
- Feeding **issues, incidents and complaints** resulting from failures in the specific agreements **into the review processes** for the individual agreements.
- **Share information free of charge** unless special charging arrangements are agreed.
- Seeking **legal advice** where appropriate.
- Ensuring that their **registration as Controllers under the DPA 2018** is adequate for the purposes for which they may need to process and share information with one another.
- Supporting the **principles of equality and diversity** within the community, including ensuring that information provided to the public is in appropriate formats and languages.

The organisations signed up to this Protocol are **fully committed to adhering to these principles** at all times.

Information disclosure & exchange

General principles

In the interests of **fairness and transparency**, partners agree to the following principles:

- The sharing of **personal information** is in a lawful manner.
- **Any shared personal data**, including special category data and criminal offence data is **in accordance with the data protection principles**, UK GDPR and Data Protection Act 2018.

The principles established by this Protocol make sure that personal information is:

- Used **fairly, lawfully** and **transparently**.[5]
- Used for **specified, explicit purposes**.
- Used in a way that is **adequate, relevant and limited** to what is necessary.

[5] Transparency is not always necessary in relation to processing for law enforcement purposes

- **Accurate** and, where necessary, kept up to date.
- Kept for **no longer than is necessary**.
- Handled and stored in a way that ensures **appropriate security**, including protection against unlawful or unauthorised processing, access, loss, destruction or damage

In addition, organisations must:

- **Respect data subject rights** and have in place appropriate technical and organisational measures to meet the requirements of accountability
- Undertake **Data Protection Impact Assessments** as appropriate
- Make available **Privacy Notices in accordance with ICO guidance** which include that this processing takes place
- Ensure staff within their organisations have undergone **training in the law of data protection**, their duty of confidentiality under the contract, and in the care of handling personal data.
- Agree to assist the Data Owner promptly with all **subject access requests** which may be received from the data subjects of any shared personal data.
- **Not use any personal data for any other purposes** other than those formally agreed by the Data Owner.
- **Not disclose any personal data to a third party** in any circumstances other than at the specific written approval of the Data Owner.
- **Not sub-contract any of the processing**, nor transfer the data to any third party, without **explicit written agreement** from the Data Owner.

The considerations around disclosure and exchange of information **apply equally to paper and electronic records**. All considerations and procedures around the secure exchange and principles of evaluation of requests and retention of information in this ISP apply to all exchanges, irrespective of medium.

Personal and special category information shared electronically under this protocol should be shared through **secure and encrypted email** between signatories.

All requests for information should be responded to in a timely manner.

Legal powers for sharing information

The **Crime and Disorder Act 1998** is the principal Act that provide the legal power for sharing information for the purposes of community safety:

- **Section 17** imposes a duty on each responsible authority to **consider the impact** that their work may have on **crime and disorder**, the problem use of **drugs and alcohol** and **serious violence** and the need to do all that it reasonably can to prevent and reduce these issues.
- In addition, under **Section 17A**, a 'relevant authority' is under a duty to share with all other relevant authorities **prescribed**[6] **depersonalised information**

[6] As amended by the Police and Justice Act 2006. Information is of a prescribed description if it is depersonalised and listed in the Schedule to the 2007 Regulations; this is supported by the Delivering Safer Communities guidance.

which is relevant to the reduction of crime and disorder, including anti-social behaviour. A list of agreed datasets for Cornwall is provided at Appendix 4.

- **Sections 5 and 6** impose a general duty upon responsible authorities to **formulate and implement strategies** for the local area to:
  - Reduce **crime and disorder**, including anti-social and other behaviour adversely affecting the local environment
  - Combat the misuse of **drugs, alcohol and other substances**
  - Reduce **re-offending**[7] by adults and young people
  - Prevent and reduce **serious violence**[8]
- **Section 115 provides a legal gateway for sharing of personal data** by the police, local authorities, fire and rescue services, integrated care boards, probation and housing associations for the purposes of preventing future crime and disorder and to facilitate multi-agency strategies.

There are other legal powers that enable or require information to be shared, however (see Appendix 2 for a non-exhaustive list of legislation).

Lawful basis to share information

Any sharing of personal data including sensitive data known as special category data or criminal offence data must be undertaken in accordance with **UK GDPR and Data Protection Act 2018** (see Appendix 2 DPA 2018 and GDPR for more information).

Shared personal data will usually include information about the nature of the issue and, where relevant, personal data such as names, addresses and dates of birth of offenders, victims or witnesses. Most of the shared personal data will also include **sensitive/special category/criminal offence personal data** as defined in data protection legislation. Sharing of this type of sensitive information is **allowed in lawful and appropriate circumstances**.

In order to share appropriate information between partners there must be **a lawful, defined and justifiable purpose**(s), which supports the effective delivery of a policy, or service that respects people's expectations about the privacy and confidentiality of their personal information but also considers the consequences of a failure to act.

Law enforcement processing

Part 3 of the DPA 2018 sets out the requirements for the **processing of personal data for criminal 'law enforcement purposes'**. The ICO has produced a detailed Guide to Law Enforcement Processing.

Part 3 applies if you process personal data for 'law enforcement purposes', although it is unlikely to apply to all processing that you do. It covers processing for the **prevention, investigation, detection or prosecution of criminal offences**, or the execution of criminal penalties, including the **safeguarding against and the prevention of threats** to public security.

[7] As amended by the Policing and Crime Act 2009
[8] As amended by the Police, Crime, Sentencing and Courts Act 2021

Information sharing within multi-agency meetings

Signatories to this protocol understand that shared **personal data will be shared at multi-agency meetings**.

For example, there may be meetings between members of staff from **different agencies sharing information about a common case** in order to build a foundation of accurate knowledge and evidence, to **minimise the risk of harm** to the community, whilst allowing **proper management** of the case. The intention of this Protocol is to cover all such information sharing.

Information **may be legally shared without consent** about any person or group of people who **pose a risk of harm** to the community, other individuals or professionals.

If any shared personal **data relates to an ongoing investigation or prosecution** by any of the agencies then consultation must take place with the **investigating officer and Crown Prosecution Service** as the matter will be sub-judice. This will ensure that disclosure will not adversely prejudice the outcome of the matter.

Using the **Government Security Classifications**, the chair of each meeting should designate the level of confidentiality appropriate to the information shared at the outset (see Appendix 3).

Where relevant, they must provide a **confidentiality declaration sign-in sheet** (Appendix 6) which states the data sharing requirements relevant to the meeting and **highlight the restrictions or limitations** in relation to the use of the information.

If used, the **chair should securely retain a copy** of this confidentiality declaration sign-in sheet.

The parties to this protocol understand that in keeping with government initiatives to invite a **wider spectrum of organisations** to assist the relevant authorities to implement the Crime and Disorder Act 1998, it is likely that there will be representation from **organisations that are not signatories** to this protocol.

To allow for this, the signing-in sheet should state that the signatory agrees to abide by all the terms of this Protocol. It is **good practice to use the Government Security Classifications** (see Appendix 3). These set out levels of confidentiality and appropriate security measures that should be applied to information assets.

These classifications are the method by which the originator of an asset (all material assets, i.e. papers, drawings, images, disks and all forms of electronic data records) indicates to others **the levels of protection required when handling the asset** in question. This includes terms of **sensitivity, security, storage, movement** both within the guidance and outside the originator's own department or force and its ultimate **method of disposal**.

Information sharing outside meetings

This Protocol is to **facilitate the exchange of information between partners**. It is, however, incumbent on all partners to recognise that any information shared must be justified on the merits of each case.

Personal information must be requested in a legally compliant manner, setting out the legal grounds for disclosure, for example if the Crime and Taxation exemption under the Data Protection Act (DPA) 2018 Schedule 2 Part 1 (2) is being relied on, then this should be formally set out and the specific details required. Where relevant, use access request forms, or alternative official third party subject access request forms (where required by other partners).

Privacy Notices should make clear where sharing of information will occur. Information shared should only be used for the purpose requested by the requesting partner and **should not be shared further without consent of the information owner** unless there is a legal obligation or other lawful basis for doing so.

Any sharing and storing of data must be in accordance with the relevant legislation. In particular, when sharing personal data, use a secure transmission system, such as secure email or courier or hosted on a secure system shared by partners. All Partner agencies must have **appropriate technical and organisational measures in place**, having regard to the nature and sensitivity of the information, to ensure information security.

This will include **monitoring and auditing procedures** as well as the ability to respond to any failure to adhere to the data sharing Protocol swiftly and effectively and to report any personal data breach. **Only keep information as long as it is necessary**. All signatories must confidentially destroy the information in accordance with any relevant data retention and disposal policies.

Amethyst Community Safety Intelligence Team

Based within Cornwall Council's Community Services, the Amethyst **Team supports evidence-based delivery** in all aspects of community safety business for Safer Cornwall and the Council. The team specialises in **data analysis and research** relating to crime, anti-social behaviour, problem use of alcohol and other drugs, reoffending and other issues impacting on community safety in Cornwall.

Amethyst delivers the **statutory Community Safety Strategic Assessment** and other statutory and non-statutory intelligence products. The team also **manages performance** for the Partnership.

- Amethyst receive and process the prescribed datasets detailed at Appendix 4 where these are provided by the relevant partners.
- Depersonalised and aggregated data is drawn from the responsible authorities to generate collective information to identify **patterns and trends**, understand **need and demand** and assess the **effectiveness of responses** in place.
- Depersonalised and aggregated data is drawn from the responsible authorities to develop, maintain and monitor an **agreed set of performance measures**, for the overarching Partnership Plan and for the thematic strategies that sit underneath the Partnership Plan umbrella.
- Amethyst **staff are police vetted** to Level 2.

Police threat and risk documents

These documents produced by Devon and Cornwall Police may contain **sensitive personal information** relating to victims and offenders, which include vulnerable adults, children and young people. Documents produced to inform strategic tasking are vital documents in identifying any risks relating to vulnerable individuals that can be brought to the attention of the appropriate agency.

Any such **documents are protectively marked** as 'restricted' and will be shared, via secure e-mail, with appropriate officers from Cornwall Council (Community Safety and Safeguarding).

If **hard copies** of the documents are produced, they must be **kept in locked storage** following the general principles for secure information exchange, storage and retention outlined in the Protocol.

Security

General principles

Ensuring that personal information is protected against accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access is the **sixth principle of the UK General Data Protection Regulations** (UK GDPR).

All partners shall employ **appropriate operational and technological processes and procedures** to keep the personal data safe from unauthorised use or access, loss, destruction, theft or disclosure. The organisational, operational and technological processes and procedures adopted are required to comply with either the **NHS Data Security and Protection Toolkit**, or the requirements of **ISO/IEC 27001:2005** (ISO/IEC 17799:2005) as appropriate to the services provided.

Information shared by Partners will be held securely. Electronic copies of information will only ever be held on encrypted devices or servers and will not be emailed outside of the organisation. **Only nominated representatives** will be able to access, request information and make disclosure decisions.

Article 32 of the UK GDPR includes encryption as an example of an appropriate technical measure, depending on the nature and risks of your processing activities.

Any staff who hold **information on a portable device** (e.g. laptop, USB stick) must ensure that **the device is owned or approved** (via *Bring Your Own Device* schemes) by their organisation, that it is **password protected** to comply with the standards of their own organisation's procedures and that it uses **the approved encryption software** of their respective organisation.

A business case may be required to permit use of removable media, dependent on the policy of partner organisations.

Partners processing information under this agreement are responsible for ensuring that **all devices used for remote working are encrypted** (laptops, smart phones, tablets, drives or removable electronic media) using a solution that means current standards.

Paper copies of information will be held securely (including print outs of electronic information); transferred by courier in sealed containers and shredded upon disposal and buildings and areas where personal data can be accessed from must have **adequate physical security** in order to prevent unauthorised access.

All partners will ensure that the **personal data is securely removed from their systems** and any printed copies securely destroyed **at the end of the work** for which it was intended, or on termination of the contract.

In complying with this clause, **electronic copies of the personal data shall be securely destroyed** by either physical destruction of the storage media or secure deletion using appropriate electronic shredding software that meets HM Government standards. **Any hard copies will be destroyed** by cross-cutting shredding and secure recycling of the paper waste.

Secure exchange of information

Unguarded exchange of personal information may not only **infringe the rights of the individual subject** or others that may be identifiable from the information, but also **compromise the organisations sharing information** or jeopardise any proceedings or legal measures based upon that information.

Electronic exchange can be the most secure and auditable means of exchanging information provided this is **done using suitably secure technology**. Personal information should only be exchanged electronically using a **secure and encrypted messaging system** such as the public service network or Transport Layer Security.[9]

Transport Layer Security (TLS) is a protocol which provides **privacy between communicating applications** and their users, or between communicating services. When a server and client communicate, well-configured TLS ensures that no third party can eavesdrop or tamper with any message.

Examples of **secure email addresses** include emails between the following:

- gov.uk
- pnn.police.uk
- nhs.net
- justice.gov.uk

Cornwall Council IS have applied the **government's secure email standard** to their Office 365 system. The Council has a list of **trusted domains** held on the intranet – however this is **only accessible internally** by Cornwall Council staff.

Do not send any personal or special category data via external email to any email address that is not in a trusted domain. If you need to send sensitive documents to another organisation **other methods can be used, such as Egress Switch**.

It is it is for each organisation to ensure that information is transferred securely. If you are unsure whether an email exchange is secure, please contact your ICT Security department to clarify.

[9] https://www.ncsc.gov.uk/guidance/tls-external-facing-services

Retention & disposal

Partners must **comply with their own agencies' retention and disposal policies**. These should cover both electronic and paper based information.

Data breaches

A personal data breach means a **breach of security relating to personal data** that has resulted in the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, the data.

All agencies who are party to this Protocol must have in place **appropriate measures to investigate and deal with personal data breaches** (both accidental and deliberate). The **agency must inform all affected partners** of the data breach immediately to enable them, where relevant, to meet their legal duty under UK GDPR to **report personal data breaches within 72 hours** to the Information Commissioner.

Partner agencies must follow the guidance of the Information Commissioner' Office on personal data breaches – see https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/

The **partner organisation where the breach has occurred shall conduct a full investigation** of the breach and share the findings with the other relevant partners and the Safer Cornwall Strategic Board.

Implementation, monitoring & review

All of the signatories own the Protocol. This document is an over-arching code of behaviour for all information-sharing applications, supplemented by Information Sharing Agreements (ISAs) for specific purposes. **ISAs will adopt the principles and commitments in the Protocol** as their base line and identify any additional service specific requirements.

A **review of the Protocol will be undertaken annually in March** and the document updated to account for any changes in legislation and developments in national guidance. Issues arising from breaches of the Protocol, changes in legislation, or recommendations arising from review may result in an earlier review.

Each partner organisation will be individually responsible for monitoring and reviewing the implementation of the Protocol and publishing any individual Information Sharing Agreements they may have.

Any of the signatories can request an extraordinary review at any time when a joint discussion or decision is necessary to tackle local service developments. Work to develop individual ISAs will be the responsibility of the organisations wishing to share information as will the review of existing ISAs on updates to the Protocol, ISA Template (Appendix 5) and changes to relevant legislation.

Access to information & mutual assistance

Individual's rights to their data will be **managed through processes compliant with the Data Protection Act 2018**, Chapter 12, Sections 45-48. The right to request access or erasure may be refused where the Health, Education or Social Care data tests are met.

Each partner organisation will **follow their own procedures** when Data Subject Access Rights are requested and shall **assist each other in complying** with all applicable requirements of the Data Protection Legislation.[10]

If a partner organisation receives a subject access application, they need to consider whether the information can be provided, or whether an exemption under the Data Protection Act needs to be applied to enable the request to be denied.

The exemption most likely to apply in the context of this protocol is where disclosure would be likely to **prejudice the prevention or detection of crime** or the apprehension or prosecution of offenders.[11]

In particular, each party shall:

- Consult with the other partners about **any notices given to data subjects** in relation to the shared personal data.
- **Promptly inform the other partners** about the receipt of any data subject access request.
- **Provide the other partners with reasonable assistance** in complying with any data subject access request
- **Not disclose or release** any shared personal data in response to a data subject access request **without first consulting the partner from where the information originated**, wherever possible
- Assist the other partner, in responding to any request from a data subject and in ensuring compliance with its **obligations under the Data Protection Legislation** with respect to security, breach notifications, impact assessments and consultations with supervisory authorities or regulators.
- Notify the other partner without undue delay on becoming aware of any **breach of the Data Protection Legislation.**
- **Maintain complete and accurate records** and information to demonstrate its compliance with this clause.

Complaints

Partner organisations must have **procedures in place to address complaints** relating to the inappropriate disclosure of information.

[10] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/
[11] DPA 2018, Schedule 2, Part 1, Paragraph 2

All partner organisations agree to **cooperate in any complaint investigation** where they have information that is relevant to the investigation. Partners must also ensure that their complaints procedures and the contact details of the Data Protection Officer (DPO) are well publicised for this purpose.

If the complaint affects more than one partner organisation it should be brought to the attention of the **appropriate complaints officers/DPOs** who should liaise to investigate the complaint.

Partner organisation non-compliance

In the event of a **suspected failure** within their organisation to comply with this agreement, partner organisations will **carry out and record an adequate investigation**.

If the partner organisation finds there has been a failure it will ensure that:

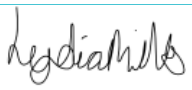
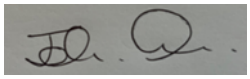
- If one partner organisation believes another has failed to comply with this agreement it should **notify the other partner organisation in writing**, giving full details. The other partner organisation should then **investigate the alleged failure**.
- If it finds there was **no failure** it should notify the first partner organisation in writing giving its reasons.
- Where it is clear that a partner organisation is **not complying with this Protocol**, other partners may decide to **stop sharing information** until the issues are resolved. More information about information sharing is available here from the Information Commissioner.
- **Partner organisations will make every effort to resolve disagreements** between them about personal information use and sharing. However, they recognise that ultimately each organisation, as Data Controller, must exercise its own discretion in interpreting and applying this Protocol and ensuring compliance with the data protection legislation.
- **Notify nominated representatives at an early stage** of any suspected or alleged failures in compliance or partner disagreements relating to their organisation.

Authorised signatory form

COMMUNITY SAFETY INFORMATION SHARING PROTOCOL

Signatories to this agreement are:

Partner Organisation	Signatory Name & Title	Date
Cornwall Council	 Simon Mould Head of Resilent Communities	10/01/24
Cornwall Fire & Rescue Service	 Antony Bartlett – Assistant Chief Fire Officer	09/03/24
Cornwall and Isles of Scilly Youth Justice Service	 Ben Davies, Service Director Children and Family Services	12/01/24
Devon and Cornwall Police	 C/Supt Ben Deer Vice Chair, Safer Cornwall	27/03/2024
NHS Cornwall and Isles of Scilly Integrated Care Board	 Susan Bracefield, Chief Nursing Officer	26/03/24
Probation Service	 Jonathan Nason, Head of Cornwall and IOS PDU	12/01/24
Office of the Police and Crime Commissioner for Devon, Cornwall and Isles of Scilly	 Frances Hughes, CEO, OPCC Devon & Cornwall & Isles of Scilly	19/03/24
South Western Ambulance Service NHS Foundation Trust	 Dr Matt Thomas Executive Medical Director and Caldicott Guardian	20 May 2024

Partner Organisation	Signatory Name & Title	Date
Department for Work and Pensions	 Emma Benning Advanced Customer Support Senior leader. Devon & Cornwall	14/03/24
Office for Health Improvement & Disparities	 Ian Keasey, Population Health and Wellbeing Programme Manager, OHID	27/03/24
Cornwall Association of Local Councils	 County Executive Officer	11/01/2024
Voluntary Sector Forum	 Emma Rowse, Chief Executive Officer, Cornwall Voluntary Sector Forum	15/01/24
Safer Stronger Communities	 Lydia Mills, CEO	19/03/24
Safer Scilly	 Russell Ashman Chief Executive Council of the Isles of Scilly	14.03.2024
Our Safeguarding Children Partnership for Cornwall and the Isles of Scilly	John Clements – Independent Chair 	11 March 2024
Cornwall and Isles of Scilly Safeguarding Adults Board	 Fiona Field, Independent Chair, Cornwall and Isles of Scilly Safeguarding Adults Board	12/03/24

APPENDICES

Appendix 1: Definitions

Crime

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.[12]

Anti-social behaviour

Anti-social behaviour is defined as 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.

Disorder

Disorder refers to the level or pattern of anti-social behaviour within a particular area.

Incident

An incident report is any communication, by whatever means, about a matter that comes to the attention of the police. All reports of incidents, whether from victims, witnesses or third parties, and whether crime-related or not, result in the registration of an incident report by the police. An incident is recorded as a crime if, on the balance of probability, the circumstances as reported amount to a crime defined by law and there is no credible evidence to the contrary.

Depersonalised (Non personal or anonymised) information

Depersonalised information is defined as information where any reference to or means of identifying a living individual has been removed. This is any information, which does not (or cannot be used to) establish the identity of a living individual. There are no legal restrictions on the exchange of anonymised information.

Information in the public domain

This type of information incorporates any information, which is publicly available, whether it relates to an individual or not.

Personal data

Personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is 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.

Pseudonymised Information

Information that is processed in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not

[12] The term penalty refers to any punishment fixed by law

attributed to an identified or identifiable natural person. Personal data which have undergone pseudonymisation, which could be attributed to a natural person by the use of additional information should be treated as personal data.

Special Category Data

Special category data is 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.

Although not defined under Data Protection legislation as special category data, for the purpose of this protocol the following categories should be processed in the same way as special category data:

- Information relating to people who have experienced crime directly
- Information relating to witnesses of crime

Appendix 2: Legal framework

The legal framework for sharing information

Crime and Disorder Act 1998

The **Crime and Disorder Act 1998** is the principal Act that provide the legal power for sharing information for the purposes of community safety. The relevant sections of the Act are described in the Legal powers for sharing information section in the main body of the Protocol.

There is a wide range of activities in which the sharing of personal information is not only useful but legally permissible, particularly where decisions regarding particular interventions with individuals are being discussed. This power however does not override other legal obligations such as compliance with the Data Protection Act 2018, the Human Rights Act (1998) or the common law of confidentiality.[13]

Criminal Justice and Court Services Act 2000

This Act provides for a specific duty for the Police and Probation Services to make joint arrangements for the **assessment and management of the risks posed by sexual, violent and other offenders** who may cause serious harm to the public.

Police and Justice Act 2006

This Act introduces a **duty to share depersonalised information** which is intended to increase the effectiveness of partnerships by ensuring that they have the necessary multi-agency information for identifying **priorities**, mapping **trends** and **patterns** in crime and disorder, and **managing their performance**. This duty only applies when the authority holds the information so it **does not require the collection of any additional information**. In each case, the duty applies to information relating to the partnership area as defined by the district or unitary authority area. The specified information sets are listed in Appendix 3.

The Police and Justice Act 2006 also places a statutory duty on the Strategic Boards of all CSPs to prepare an **information sharing protocol**.[14] The protocol must cover the sharing of information under the new duty to **share specified depersonalised datasets** and also any additional information sharing between the responsible authorities and other agencies named under Section 115 of the Crime and Disorder Act 1998, including **personal information**. A statutory duty has also been placed on each responsible authority to nominate a **designated liaison officer** whose role is to facilitate the sharing of information with other partners.

Police, Crime, Sentencing and Courts Act 2021

This Act introduces the **Serious Violence Duty**, which commenced on 31st January 2023.

As a result of this duty the police, local authorities, fire and rescue authorities, and specified health and criminal justice agencies have to work together to identify and publish what actions they need to take collectively to reduce violent crime, including domestic abuse and sexual offences. Educational authorities, prisons and youth

[13] The Human Rights Act is now applied to the common law under the law relating to the misuse of private information (see 2.2 and 2.3)
[14] Statutory Instrument 2007/1830 part 4 (1) and (2) require the drafting of an Information Sharing Protocol

custody agencies may also be required to work with those bodies as a result of this duty.

The **legislation grants these authorities the power to share data and information** with each other for the purpose of preventing and reducing serious violence. The **emphasis is on early intervention with young peopl**e in order to prevent them from becoming either a victim or perpetrator of serious violence in the first place.

Other relevant Acts

Whilst the legislation highlighted above are the principle Acts covering the exchange of information in respect of crime and disorder, there are a wide range of other Acts that require or enable (subject to the wider law) the sharing of information, including:

- Children Act 1989
- Children Act 2004
- Domestic Violence Crime and Victims Act 2004
- Anti-Social Behaviour Act 2003
- Sexual Offences Act 2003
- Local Authority and Social Services Act 1970
- Housing Act 1996
- Housing Act 2004
- Police and Criminal Evidence Act 2001
- Serious Crime Act 2015
- Anti-Social Behaviour, Crime and Policing Act 2014
- Counter Terrorism and Security Act 2015
- Serious Violence Duty 2021
- Domestic Abuse Act 2021
- Police and Social Responsibility Act 2011

Legislation governing the sharing of information

Data Protection Act 2018 ('the DPA')/General Data Protection Regulations

Personal data can only be 'processed' (obtained, recorded, held, used, shared, deleted, etc.) if there is a lawful basis for doing so.

The lawful bases that are **most likely to apply** in the context of this protocol are under Article 6 and Article 9 of the UK GDPR (Schedule 9 and 10 of DPA 2018):

- Article 6.1(c) - processing necessary for compliance with a legal obligation
- Article 6.1.(e) - processing necessary for the performance of a public interest task
- Article 6.1 (e) - the exercise of official authority

In addition, for **special category** the lawful bases that are most likely to apply

- Article 9.2 (a) explicit consent and
- Article 9.2 (g) processing necessary for reasons of substantial public interest

Or

- There must be an **exemption under the DPA for processing the data**. These can be used on a case by case basis and includes exemptions for the apprehension and prosecution of offenders (Schedule 2 part 1 of the DPA 2018) and prospective legal proceedings (Schedule 2 part 5 of the DPA 2018)

Data relating to criminal convictions and offences and to security measures is also regarded as being particularly sensitive but it is treated separately from special category data. In addition to an Article 6 basis, one of the conditions in Part 1, 2 or 3 of Schedule 1 of the DPA must be met (DPA, Section 10).

So **criminal convictions and offences data** (which includes information about the alleged commission of offences)[15] can be processed for a wide range of purposes. However, the conditions that are most likely to apply in the context of this protocol are that the **processing is necessary to prevent or detect unlawful acts**,[16] to protect the public against dishonesty or malpractice,[17] to comply with regulatory requirements relating to unlawful acts or dishonesty,[18] and to prevent fraud.[19] All of this processing is **based on public interest**.

Processing in the public interest, whether of special category data or criminal convictions and offences data, **should only be undertaken when seeking consent would prejudice the aim** pursued or consent cannot reasonably be obtained for other reasons.[20]

Moreover, the **public interest must be 'substantial'**.[21] That means the processing must be '*proportionate to the aim pursued, respect the essence of the right to data protection, and provide suitable and specific measures to safeguard the fundamental rights and interests of the data subject*'.[22]

However, processing (including recording, using and disclosing) **personal data for the prevention or detection of crime or the apprehension or prosecution of offenders is exempt** from the DPA's Data Protection Principles and data subject rights to the extent that the application of those provisions would be likely to prejudice those purposes. The focus of the exemption is prejudice to crime prevention, etc., and not the rights of the data subject. The threshold for sharing information under the exemption is lower than for sharing in the public interest.

Human Rights Act 1998

This Act should be taken into account in establishing whether the purpose of information exchange is lawful.

The Human Rights Act 1998 gives further effect in domestic law to **Articles of the European Convention on Human Rights** (ECHR). The Act requires all domestic law to be compatible with the Convention Articles. It also places a legal obligation on all public authorities to **act in a manner compatible with the Convention**.

[15] DPA 2018, section 11(2)
[16] DPA 2018, Schedule 1, Part 2, paragraph 10
[17] DPA 2018, Schedule 1, Part 2, paragraph 11
[18] DPA 2018, Schedule 1, Part 2, paragraph 12
[19] DPA 2018, Schedule 1, Part 2, paragraph 14
[20] DPA 2018, Schedule 1, Part 2, paragraphs 10,11,12 and 14
[21] As above
[22] GDPR, Article 9.2(g)

Should a public authority fail to do this then it may be subject to a legal action under section 7 of the Act. This obligation should not be seen solely in terms of an obligation not to violate Convention Rights but also as a positive obligation to uphold these rights.

Article 8 of the Act is of particular relevance to information sharing as this relates to *'the right to respect for private and family life'*.

Common law duty of confidentiality

The duty of confidentiality has been defined by a series of legal judgements and is a **common law concept rather than a statutory requirement**. Personal information which is seen as subject to this duty includes information that:

- Is not already in the public domain.
- Has a certain degree of sensitivity.
- Was provided on the expectation that it would only be used or disclosed for particular purposes (this applies to both the living and the dead).

Common Law judgements have identified a number of exceptions:

- Where there is a legal compulsion to disclose.
- Where there is an overriding duty to the public, this includes the need to prevent, detect and prosecute serious crime.
- Where the person to whom the information refers has consented.

Where information is held in confidence e.g. as is the case with personal information provided to the National Health Service and medical practitioners by patients, the **consent of the individual concerned should normally be sought** prior to information being disclosed.

Where **consent is withheld or unobtainable**, designated officers should assess, on a case-by-case basis, whether **disclosure is necessary to support action under the Crime and Disorder Act** and whether the public interest arguments for disclosure are of sufficient weight to over-ride the duty of confidence.

The 8 Caldicott Principles

The Caldicott Principles are **guidelines that are followed by Social Care and Health professionals** regarding the use of person-identifiable and confidential information.

Established following the 1997 Caldicott Committee Report, there are six general principles for the **safe handling of personal-identifiable information**, that provide the guidelines to which the NHS works. They work hand-in-hand with the Principles of the Data Protection Act 2018.

The 8 principles are:
1. Justify the purpose(s).
2. Don't use personal confidential data unless it is absolutely necessary.
3. Use the minimum necessary personal confidential data.
4. Access to personal confidential data should be on a strict need-to-know basis.

5. Everyone with access to personal confidential data should be aware of their responsibilities.
6. Comply with the law.
7. The duty to share information can be as important as the duty to protect patient confidentiality.
8. Inform patients and service users about how their confidential information is used.

Each health and social care organisation has a Caldicott Guardian responsible for:

- Agreeing and reviewing information sharing policy.
- Ensuring the organisation satisfies the highest practical confidentiality standards.
- Acting as the conscience of the organisation.
- Advising on lawful and ethical processing of information.
- Resolving local issues.
- Ensuring a record of resolved issues is kept.

Freedom of Information Act (2000)

Any person under the provisions of the Freedom of Information (FOI) Act **may request information** held by public sector authorities.

Under certain circumstances an authority **may refuse to supply information** because they believe that **one or more of 24 possible exemptions may apply** to the information being requested.

For example, disclosure may breach other legislation such as the Data Protection Act or the information may already be widely available in the public domain. Unless these exemptions apply, **public authorities are obliged to provide the information within 20 working days** of the receipt of a request.

Since the Data Protection Act continues to govern access to personalised information, it is mainly non-personal information that is affected by the provisions of the FOI. This will include information in any form, including informal, electronic and database records. The FOIA is a complex piece of legislation. Almost all authorities have trained specific staff to deal with applications for information made under the Act. Their advice should be sought in the event of any questions arising about the Act.

A request may be received by an authority for **any information that it holds**, not just that which it has generated itself or relates to its own activity. Should a request under FOI be received by one authority for **information which originated with another authority**, it is a requirement of this Protocol that the originating authority is **consulted before any release is made**.

Appendix 3 Information Classification Scheme

The Government Security Classifications Policy provides an administrative system to protect information assets appropriately against prevalent threats.The Government Security Classification system has three levels: Official, Secret, and Top Secret.

Cornwall Council has reviewed the information classification scheme which enables officers to label Council business information. The labels form part of Cornwall Council's Information Classification Policy, which applies to all information, no matter where it is stored or what format it takes. Each label has its own protection requirements.

The two schemes are shown in the table below.

Government Classification Scheme	Cornwall Council Classification Scheme	Guidance
n/a	Public	Public information can be made freely available in the public domain and would not cause damage or harm to the Council, partners or individuals if released.
Official	Controlled	All routine public sector business, operations and services
Official	Personal	Personally identifiable information (not special category data)
Official - Sensitive	Confidential	A limited subset of Official information that could have more damaging consequences (for individuals, an organisation or government generally) if it were lost, stolen or published in the media. In cases where there is a clear and justifiable requirement to share only on a need to know basis, the Official – Sensitive classification should be used.
Secret	Confidential	Very sensitive information where compromise would directly threaten an individual's life, liberty or safety or cause serious damage to the effectiveness or security of the UK
Top Secret	Confidential	Exceptionally sensitive information assets that directly support (or threaten) the national security of the UK or allies. The chair of each multi-agency meeting is responsible for ensuring the confidentiality declaration sign-in sheet is kept current and as far as they are able to, includes all legal requirements surrounding information sharing

Appendix 4 Specific data sets

Specific depersonalised data sets (minimum requirements) to be shared under the Police and Justice Act 2006 and other recommended minimum datasets for CSPs.

Organisation	Data sets
Police	• **Depersonalised data**: **recorded offences of crime** according to the Home Office Notifiable Offences List, including sub-category, time, date and location, details of the offence, details of the accused/offender and the victim/target. Also to include recorded outcome. • **Depersonalised data**: **recorded incidents** of anti-social behaviour, transport incidents and public safety/welfare incidents, including domestic abuse related incidents, and the sub-category, time, date and location of each of those incidents. • **Depersonalised data: recorded stops and searches.** A stop may not result in a search, but as a minimum details of the search rather than all stops that do not result in a search should be shared. Including date, time and location of the search, gender, age and ethnicity of suspect, reason for search and results of search (arrest, caution, no action). • **Sensitive personalised data**: records on offenders being managed through **Integrated Offender Management** (IOM) in order to keep account of their activities and status, including age, gender, ethnicity, occupation, offences committed, current status and postcode of residence. • **Restricted data: intelligence captured in the local PREVENT Strategic Assessment** should be shared with the CSP. As a minimum this should include the current local threat, known levels of violent extremism in the local area and details of vulnerable persons, groups, communities and places that may be exploited by violent extremism.
Fire and Rescue	• **Depersonalised data: recorded fire incidents** – deliberate primary fires (excluding deliberate primary fires in vehicles), deliberate primary fires in a vehicle, deliberate secondary fires (excluding deliberate secondary fires in vehicles), fires in a dwelling where no smoke alarm was fitted attended by the fire and rescue service, and incidents of violence against employees of the fire and rescue service – including the time, date and location of each incident. • **Depersonalised data: records of calls to malicious false alarms**, including the time, date and the purported location of those alarms as defined in accordance with Fire Statistics, United Kingdom 2005. • **Depersonalised data: records of water safety incidents**, time, date and location (recommended).

Organisation	Data sets
Local Authority	• **Depersonalised data: recorded incidents of anti-social behaviour and environmental crime** reported to the council, including the category, time, date and location of incidents. These recorded incidents most commonly refer to neighbour noise nuisance, rowdy behaviour, nuisance caused by young people, graffiti, vandalism, flytipping (domestic or small scale dumping of non-domestic waste), and abandoned vehicles. • **Depersonalised data: recorded incidents of anti-social behaviour** reported to local authority housing and/or registered social landlords, including the category, time, date and location of incidents. • **Depersonalised data: road traffic collisions** – the time, date and location of each road traffic collision in the area and the number of adults and children killed, seriously injured and slightly injured in each of those collisions. • **Depersonalised data : permanent and fixed term exclusions** – information held by the local authority on the age and gender of each of the pupils subject to a permanent or fixed term exclusion from primary and secondary schools in the area, including gender, age, ethnicity, name of school and reason for exclusion.
Drug and Alcohol Action Team	• **Depersonalised data: records of adults in drug treatment** (recorded on the National Drug Treatment Service Management System), including age, gender, full postcode of residence, primary and secondary drug of use (including alcohol), referral source, type of treatment, date when treatment began, date when treatment ended and outcome. • **Depersonalised data: records of young people in drug treatment** (recorded on the National Drug Treatment Service Management System), including age, gender, full postcode of residence, primary and secondary drug of use (including alcohol), referral source, type of treatment, date when treatment began, date when treatment ended and outcome. • **Restricted data: more detailed information on adults and young people in treatment**, shared for the purposes of needs assessment.
Health ICB	• **Depersonalised data: Hospital admissions**, including date, age, ethnicity and the outward part of the postcode of the patient's address and the reason for admission/diagnosis, within the following blocks of International Classification of Diseases: a) assault (X85-Y09) b) mental and behavioural disorders due to psychoactive substance use (F10-F19) c) toxic effect of alcohol (T51) d) other entries where there is evidence of alcohol involvement determined by blood alcohol level (Y90) or

Organisation	Data sets
	evidence of alcohol involvement determined by level of intoxication (Y91). • Hospital admissions records related to domestic abuse and the date of such admissions. • Records of outpatient first attendances for mental ill health.
Ambulance Service	• **Depersonalised data: ambulance call-outs to incidents relating to crime and disorder** including the category (using any system for classifying crime and disorder used by that authority), outward part of the postcode of the location, time and date.
Probation	• **Depersonalised data: records of people under supervision** by the Probation Service, including age, gender, postcode of residence, offence description and information on the assessment of their offending in terms of their needs and future risks.
Youth Justice Service	• **Depersonalised data: records of young people engaged with the Youth Justice Service,** including age, gender, postcode of residence, offence description and information on the assessment of their offending in terms of their needs and future risks.
Prisons	• **Personalised data: Records on prisoners who reside in the local area**, with details on when they are to be released, including name, gender, date of birth, length of sentence, offence committed and address where they will reside after release.
Youth Custody Service	• **Personalised data: Records of relevant young people who reside in the local area**, with details on when they are to be released, including name, gender, date of birth, length of sentence, offence committed and address where they will reside after release.

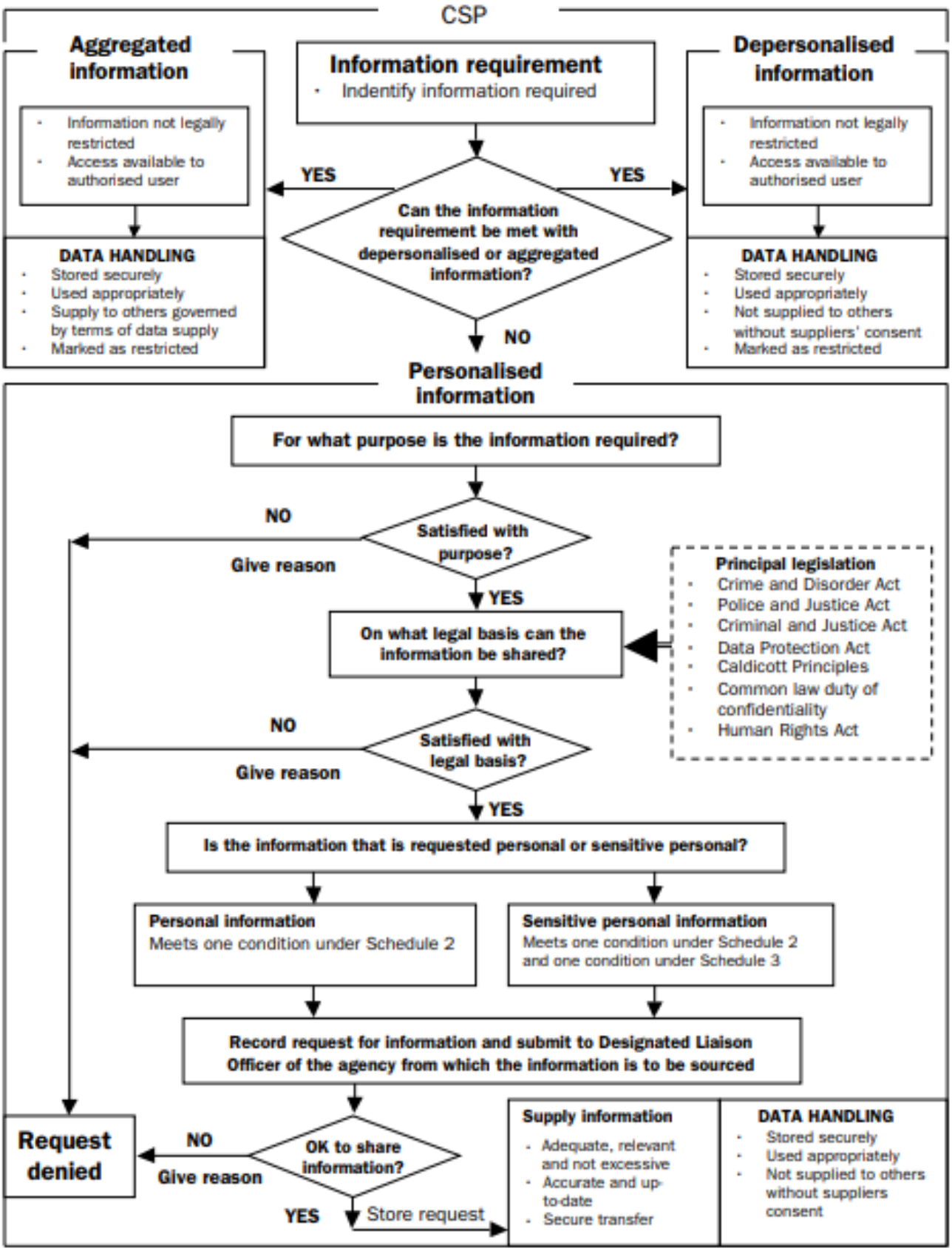
For reference, see Information Sharing Regulations (Appednix J) of the Home Office guidance Delivering community safety: a guide to effective partnership working (2007). This is expected to be updated further to the CSP Review in 2023/24.

The Police and Justice Act 2006 **specifically excludes any personal information from this duty to disclose**. This means information which can identify a living individual, either by itself or in combination with other information held, or likely to be held, by the relevant authority.

Sharing **precise location information** may, in some circumstances, be sufficient to identify a living individual. In such instances, the **Duty does not apply**. Subject to complying with other legal obligations such as the common law of confidentiality for information from ambulance callouts, the **authority may still choose to disclose this information** to the other Section 115 relevant authorities, who should treat it as **personal information**.

Alternatively, the authority may choose to share less specific location information so that the dataset contains **exclusively depersonalised information**.

Flow model summarising the processes involved in sharing information for community safety purposes (performance monitoring, intelligence development or service delivery).



Appendix 5: Information Sharing Agreement template

Information Sharing Agreement

[insert purpose of sharing / project title here]

Date DD/MM/YY or version

Version history				
Date	Version	Author/Editor	Comments	Approved by

This Agreement outlines the circumstances when information sharing can occur and provides a framework for achieving this appropriately and in a lawful and justified manner.

Its purpose is to facilitate the lawful exchange of information (including personal information) between the Owner and the Partner in order to support the partnership's Purpose as specified below.

This agreement should be read in conjunction with the Information Sharing Protocol to which it is appended *[add relevant ISP details and link]*

Date agreement comes into force
Indicate timescales for this agreement, including termination date if applicable.

Data controller of data to be shared
See ICO guidance for further information

Data controller relationship
See ICO guidance for further information

☐ Joint

☐ Separate

List data processors of data to be shared
See ICO guidance for further information

Purpose of sharing
Explain the specific aims of the sharing, why the sharing is necessary and the benefits you hope to bring to individuals / society

Lawful basis for sharing – please state which
See ICO guidance for further information

If lawful basis is consent, how was this obtained, how long is it valid, what processes are in place if consent is withdrawn?

☐ N/A

Which legal power for sharing applies (if applicable) - please state Act and relevant section

Who is the data about?

What data will be shared?
List data to be shared

Does the data include special category data (or sensitive processing under part 3 of the DPA 2018)?

☐ Yes
☐ No

Personal identifiable health and social care data for planning and / or research purposes - has the National Data Opt-Out been applied?

☐ Yes
☐ No
☐ N/A

Describe arrangements for secure transfer of data

Describe arrangements for the security of data

All partners shall employ appropriate operational and technological processes and procedures to keep the personal data safe from unauthorised use or access, loss, destruction, theft or disclosure. The organisational, operational and technological processes and procedures adopted are required to comply with either the NHS Data Security and Protection Toolkit, or the requirements of ISO/IEC 27001:2005 (ISO/IEC 17799:2005) as appropriate to the services provided.

Information shared by Partners will be held securely. Electronic copies of information will only ever be held on encrypted devices or servers and will not be emailed outside of the organisation. Only nominated representatives will be able to access, request information and make disclosure decisions.

Any staff who hold information on a portable device (e.g. laptop, USB stick) must ensure that the device is owned or approved (via Bring Your Own Device schemes) by their organisation, that it is password protected to comply with the standards of their own organisation's procedures and that it uses the approved encryption software of their respective organisation.

A business case may be required to permit use of removable media, dependent on the policy of partner organisations.

Partners processing information under this agreement are responsible for ensuring that all devices used for remote working are encrypted (laptops, drives or removable electronic media) using a solution that means current standards.
Paper copies of information will be held securely (including print outs of electronic information); transferred by courier in sealed containers and shredded upon disposal and buildings and areas where personal data can be accessed from must have adequate physical security in order to prevent unauthorised access.

All partners will ensure that the personal data is securely removed from their systems and any printed copies securely destroyed at the end of the work for which it was intended, or on termination of the contract.

In complying with this clause, electronic copies of the personal data shall be securely destroyed by either physical destruction of the storage media or secure deletion using appropriate electronic shredding software that meets HM Government standards. Any hard copies will be destroyed by cross-cutting shredding and secure recycling of the paper waste.

Duration and frequency of sharing

Describe arrangements for retention / deletion / return of data

Other Data Protection requirements

The Partner Organisation(s) agrees to assist the Data Owner promptly with all subject access requests which may be received from the data subjects of the personal data.

The Partner Organisation shall not use the personal data for any other purposes other than those formally agreed by the Data Owner.

The Partner Organisation shall not disclose the personal data to a third party in any circumstances other than at the specific written approval of the Data Owner.

The partner organisation is not permitted to sub-contract any of the processing, nor transfer the data to any third party, without explicit written agreement from the Data Owner.

The Partner Organisation shall ensure that all employees used by it to provide the services as defined in the Agreement have undergone training in the law of data protection, their duty of confidentiality under the contract, and in the care of handling personal data.

What are the arrangements for complying with individuals' information rights (right of access, right to object, right of rectification and erasure)?
All controllers remain responsible for compliance even if processes are in place regarding who carries out particular tasks

Has a Business and Privacy Impact Assessment been completed?

☐ Yes - Date:
☐ No

Review and monitoring arrangements

Declaration of Acceptance & Participation

In respect of [title of agreement]

By signing this agreement, all signatories accept responsibility for its execution, agree to ensure that their staff and personnel are trained so that requests for information and the process of sharing are sufficient to meet the purpose of this agreement and agree to put into practice the principles of the [name of relevant Information Sharing Protocol].

The agencies signing this agreement accept that the procedures laid down in this document provide a secure framework for the sharing of information between

agencies in a manner compliant with their statutory and professional responsibilities.

Signed by, for and on behalf of:

Organisation	
Name	
Position	
Telephone Email	
Signature	
Date	
Data Protection Officer's contact details	

Appendix 6 Confidentiality declaration

I understand that information coming into my possession or knowledge is as a consequence of the **Safer Cornwall Information Sharing Protocol**.

The information that I receive will be **held in confidence** and **must only be used as authorised** in connection with the purposes of this process, for the prevention or detection of crime, the administration of justice or where a person or group of people poses a risk of harm to the community, other individuals at risk or professionals.

I understand that the **unauthorised communication** of any such information to any person, either verbally or in writing, could result in dismissal, termination of contract, civil liability, and/or prosecution.

Record name and date of meeting, name of person, job title, organisation, signature.

If you would like this information in another format, please contact:
Community Safety Team,
Community Services, Cornwall Council

Telephone: 0300 1234 100 email: mail@safercornwall.co.uk

www.safercornwall.co.uk