Community Safety Information Sharing Protocol

Contents

1. Background and purpose of the protocol

This Information Sharing Protocol (ISP) is owned by the Safe Durham Partnership and will be managed by the Partnerships Team Manager (Durham County Council) on behalf of the Partnership. Any enquiries about the content of the document should be directed to the Partnerships Team (safedurhampartnership@durham.gov.uk)

The absence of a protocol should not prevent sharing information. If you need to share information outside of the terms of this protocol or with agencies that are not party to this protocol you should follow local and national procedures for sharing information. The guiding rule is: if you need to share information in order to protect someone from harm or criminal activity, you must do so.

1.1 Background

The Information Commissioner's Office (ICO) upholds information rights in the public interest, promoting openness by public bodies and data privacy for individuals and this protocol conforms to the Information Commissioners Office guidance.

1.2 Purpose

The purpose of sharing information[1] within the Safe Durham Partnership is:

a) Preventing crime and disorder, anti-social behaviour and substance misuse.
b) Reducing crime and disorder, anti-social behaviour and substance misuse.
c) Countering terrorism and prevention of violent extremism
d) Apprehending and prosecuting offenders.
e) Reducing re-offending.
f) Enhancing community safety.
g) Protecting vulnerable adults and children and supporting victims including those who have experienced domestic abuse and sexual violence.

The ISP seeks to:

a) Facilitate the secure exchange of depersonalised and personal information between signatory agencies.
b) Govern the use and management of information by the Safe Durham Partnership for the purposes of developing and implementing partnership plans and tactics for crime and disorder reduction including anti-social and other behaviour adversely affecting the environment, tackling substance misuse and adult and youth offending.
c) Support the actions of the Safe Durham Partnership Multi-Agency Problem-Solving Groups (MAPS) involved in tackling crime, anti-social behaviour and substance misuse.
d) Support the sharing of personal information between agencies working with those people facing multiple disadvantage experience through the Making Every Adult Matter (MEAM) approach.
e) Assist the work of the Youth Justice Service in developing and delivering the Youth Justice Plan and working in partnership with other agencies in delivering the Youth Inclusion Programme and Youth Inclusion and Support Panels.
f) Support the development of secure information exchange in response to the Integrated Offender Management (IOM) scheme.
g) Enable the exchange of personal information between agencies dealing with cases of vulnerability, domestic abuse and violence; including Domestic Homicide Reviews and Channel.
h) Enable partnership involvement in the police intelligence structures through the secure sharing of the Forcewide Strategic Threat and Risk Assessments and involvement in the monthly police force Threat and Risk meetings.

[1] 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.

i) Support information exchange for the purposes of community fire safety.
j) Facilitate the sharing of personal information in order to prevent violent extremism, radicalisation, hate crimes and support the 'Channel' process.
k) 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.
l) Ensure that the exchange of information, including by electronic means, is undertaken securely and safely.
m) Provide guidance on the storage, retrieval and disposal of information.

This ISP may not supersede existing information sharing protocols, although partner agencies have agreed to operate under this ISP wherever possible. Information exchange for Multi-Agency Public Protection Arrangements (MAPPA), Multi-Agency Risk Assessment Conferences (MARAC), Multi Agency Safeguarding Hub (MASH) and the general safeguarding principles under Local Safeguarding Children and Safeguarding Adults arrangements are excluded from this protocol.

Agencies should ensure that they have effective data protection processes in place for responding effectively and lawfully to other requests for personal information that may be made by agencies in pursuit of their main business outside the areas covered by this protocol. Although the principles on which this ISP is based will still apply, appropriate internal procedures should also be in place.

2. Sharing Information

2.1 What is information sharing?

Information sharing involves an exchange of information between one or more individuals or agencies.

2.2 Why share information?

"Information sharing is the cornerstone of delivering shared understanding of issues and arriving at shared solutions…The right information enables partners to carry out evidence-based, targeted community safety interventions and to evaluate their impact. The improved outcome of an intelligence led, problem solving approach to community safety can only be achieved when partners have access to relevant, robust and up-to-date information from a broad range of sources."

'Delivering Safer Communities: A guide to effective partnership working' Home Office (2007)

Sharing information is fundamental to the success of any partnership plan to reduce crime and disorder, to promote community safety and tackle substance misuse. The use of good quality information and intelligence is essential in identifying and limiting the activities of those committing crime and disorder and in tackling those problems that adversely affect community safety and quality of life, including anti-social behaviour, extremism and other behaviour adversely affecting the environment. It can also help to develop effective interventions at a much earlier stage to prevent those identified as being at risk from becoming offenders or victims.

The more complete the picture of an individual's circumstances – not just contact with police or other community safety agencies, but also knowledge of support already provided by agencies or social issues, family or life stresses – the more informed and effective any intervention agreed and delivered will be.

In April 2013, Dame Fiona Caldicott reported on her second review of information governance, her report "Information: To Share or Not To Share? The Information Governance Review", informally known as the Caldicott 2 Review, introduced a new 7th Caldicott Principle.

Principle 7 - The duty to share information can be as important as the duty to protect patient confidentiality

Health and social care professionals should have the confidence to share information in the best interests of their patients within the framework set out by these principles

2.3 Benefits of information sharing

The benefits of sharing information are:

a) Better informed decision making and joined up working.
b) Improved inter-agency relationships.
c) Better profiling of crime and disorder activity to enable the more effective targeting of resources.
d) A more joined up approach to providing protection to the public.
e) Regular monitoring and evaluation of community safety initiatives.
f) Reduction in crime and disorder.

3. 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[2].

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

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

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 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

a) Information relating to victims
b) Information relating to witnesses

4. Agencies involved in information sharing (Section 5 of Crime and Disorder Act)

4.1 Responsible Authorities
Responsible authorities are under a statutory duty to ensure that key agencies come together to work in partnership in a Community Safety Partnership (CSP). Under Section 5(1) of the Crime and Disorder Act the following organisations are named as Responsible Authorities within the Safe Durham Partnership:

a) Durham County Council.
b) Durham Constabulary.
c) County Durham and Darlington Fire & Rescue Service (as amended under the Police Reform Act 2002).
d) NHS County Durham Clinical Commissioning Group (CCG) (as amended under the Health and Social Care Act 2012).
e) Probation Service (as amended under Strengthening Probation, Building Confidence).

While the term 'partnership' is applied to all those who sit round the table, legally, the responsible authorities are the only bodies or agencies under the duty to meet the regulatory requirements.

4.2 Who can be asked to co-operate?
Co-operating bodies comprise of agencies that are important in supporting the development of strategic assessments and the implementation of partnership plans. 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.

Responsible Authorities are required to work in co-operation with parish councils, NHS Foundation Trusts, proprietors of independent schools and governing bodies of an institution within the further education sector and to work closely with Drug and Alcohol Teams in two tier local authority areas. From 31 July 2007, Registered Social Landlords (in England) were made co-operating bodies with the responsible authorities of community safety partnerships. The Housing Act 2004 also amended Section 115 of the Crime and Disorder Act 1998 allowing the disclosure of information to Registered Social Landlords for the purposes associated with Section 1 of the Crime and Disorder Act which is in relation to anti-social behaviour. Responsible

Authorities are also expected to invite a range of local private, voluntary, other public and community groups including the public to become involved in partnership activity. Invitees asked to participate are drawn from agencies whose knowledge will assist CSP members to reduce crime and anti-social behaviour more effectively.

Section 5(3) of the Crime and Disorder Act provides descriptions of persons or bodies, at least one of which must be invited by the Responsible Authorities to participate in the exercise of the functions conferred by section 6 of that Act (primarily the development and delivery of a partnership strategy for the reduction of crime and disorder and tackling drug abuse).

4.3 Relevant Authorities for the purposes of Section 115

The effect of Section 115 of the Crime and Disorder Act 1998 is to allow disclosure to a "relevant authority". Relevant authorities are defined as:

a) Police forces.
b) Local authorities (such as district, borough & county councils).
c) The Probation Service North East
d) Fire and rescue authorities.
e) Clinical Commissioning Groups.
f) 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).

4.4 Partners

This ISP designates which agencies are able to share personal and depersonalised data for CSP activity:

- Durham Constabulary.
- Durham County Council (including the Youth Justice Service).
- County Durham and Darlington Fire and Rescue Service.
- NHS County Durham Clinical Commissioning Group.
- The Probation Service North East
- County Durham and Darlington NHS Foundation Trust.
- Tees, Esk and Wear Valleys NHS Foundation Trust.
- Office of the Durham Police & Crime Commissioner
- HM Prison Durham.
- East Durham Trust.

4.5 Responsibilities of signatories

It is the responsibility of signatories to ensure that:

a) They are correctly registered with the Information Commissioner for sharing personal information.
b) The data protection principles are upheld.
c) Staff in their organisation receive appropriate data protection training
d) The information shared is kept secure and confidential.
e) Information is accurate and up to date.
f) Professional ethical standards are maintained.
g) A mechanism exists by which the flow of information can be controlled and made secure ensuring integrity and confidentiality of the data
h) Appropriate staff awareness raising is provided on this protocol.
i) Adequate arrangements exist to test adherence to the protocol.
j) Records are maintained of decisions to share or withhold information.
k) All instances of non-compliance and any breaches of the ISP are addressed.
l) Only the minimum amount of information necessary for the purpose is shared.

The ISP should be signed by the Chief Officer or the Caldicott Guardian for each organisation. All signatories must ensure that the protocol is fully implemented within their organisation and should develop procedures to ensure that all staff are aware of the issues around information sharing, and all Designated Officers are conversant with the ISP and their responsibilities.

5. Information Disclosure and Exchange

5.1 General principles

Any disclosure or sharing of personal information must have regard to both common and statute law, for example defamation, the common law duty of confidence, and the data protection legislation.

All disclosures must be:

a) On a case by case basis.
b) Proportionate.
c) With a minimum amount of information necessary to achieve the purpose.
d) Only with those individuals who have a right to access the information.

Extreme care and careful consideration should be taken where the disclosure of information includes personal data relating to witnesses, victims or complainants. It is recommended that expert advice is taken where the disclosure of information would include any third party information.

Parties must comply with the Data Protection legislation. In particular parties must ensure they

- Have a lawful basis for processing personal data and special category data under Article 6 and Article 9 of the UK GDPR (Schedule 9 and 10 of DPA 2018) see Appendix 4 Section 2. The lawful bases that are most likely to apply in the context of this protocol are;
    - Art 6.1(c)c - processing necessary for compliance with a legal obligation or
    - Art 6.1.(e) - processing necessary for the performance of a public interest task or the exercise of official authority (Art 6.1(e)).

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

- Art 9.2 (a) explicit consent (Art 9.2(a)) and
- Art 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 DPA2018) and prospective legal proceedings (Schedule 2 part 5 of the DPA2018)

In addition, organisations must:

- respect data subject rights and have in place appropriate technical and organisational measures to meet the requirements of accountability
- undertaking data protection impact assessments as appropriate
- ensure staff with their organisations have received appropriate data protection training.
- make available Privacy Notices in accordance with ICO guidance which include that this processing takes place.

If information is disclosed it must be stored securely and destroyed when no longer required for the purpose for which it was provided. The underlying principle of the protocol is that the source agency will always retain ownership of the personal information it discloses to another member of the partnership. The identity of the originator must therefore be recorded against the relevant information. A recipient of such information must obtain the consent of the original data owner before making a further disclosure.

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.

In all cases, every opportunity must be sought to secure and minimise the transporting of personal and special category data. Procedures for managing documentation at multi-agency meetings should include distributing and retaining documentation within the confines of the meeting; to be destroyed immediately after that meeting.

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

5.2 Law Enforcement Processing
The DPA 2018 transposes the EU Data Protection Directive 2016/680 (Law Enforcement Directive) into domestic UK law. The Directive complements the UK General Data Protection Regulation (GDPR) and 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

5.3 Protective Marking
Where protective marking is used, the Governments Security Classification System[3] should be used for protective marking so that all agencies are using the same system. The Official-Sensitive caveat should be applied where the need to know must be rigorously enforced in accordance with the government's guidance.

5.4 Orcuma FiRST
The 'Orcuma FiRST' database was commissioned by the Safe Durham Partnership and is hosted by Durham County Council and has a separate data processing agreement. It is used to gain an understanding of emerging problems and hotspot areas where problems occur. Depersonalised data is drawn from Police, Fire and Rescue and the Council to generate collective information. This data provides the foundation of the problem solving process and:

- Provides an evidence base for priorities
- Informs the MAPS meetings and points to key taskings
- Identifies existing and emerging problems/ trends
- Provides information to task agencies to conduct further research
- Provides a means to monitor accountability
- Facilitates the improved evaluation of Time Limited projects (TLPs).

5.5 Multi-Agency Problem-Solving Groups (MAPS)
Area based MAPS consist of relevant agencies brought together to address community safety issues. As well as using depersonalised information to analyse current trends and hotspot locations, these groups discuss and agree action to reduce the negative effect that problem

[3] https://www.gov.uk/government/publications/government-security-classifications

individuals and families associated with antisocial behaviour or criminality have on the wider community. Examples of issues dealt with include persistent criminal or anti-social behaviour, race/hate crime, misuse of alcohol or drugs and vulnerable people e.g. street drinkers or the homeless.

5.6 Horden Together Partnership

An element of this partnership involves working intensively with a small cohort of individuals utilising the Making Every Adult Matter (MEAM) framework. MEAM is a multi-agency approach with local partners working together to manage adults who face a multiple disadvantage experience with a combination of problems including homelessness, substance misuse, contact with the criminal justice system and mental ill health. They fall through the gaps between services and systems, making it harder for them to address their problems and lead fulfilling lives.

The MEAM approach focuses on creating long-term sustainable change to the way that complex problems and systems are approached and understood. It helps local areas design and deliver better co-ordinated services to support those with multiple disadvantage and complex needs.

It starts with partnership, co-production and vision to agree a shared understanding of the problem and vision for the whole area. It considers seven principles which can be adapted to local needs and circumstances:

- Partnership, co-production and vision
- Consistency in selecting a caseload
- Co-ordination for clients and services
- Flexible responses for services
- Service improvement and workforce development
- Measurement of success
- Sustainability and systems change

This approach makes the most of local resources and opportunities when supporting people to make lasting change to their lives and changes the level of outputs (ASB/Crime) so reducing demand on services (especially those in response).

5.7 Domestic Homicide Review and Firearms Licensing Information Exchange

Overall responsibility for establishing a Domestic Homicide Review rests with the local Community Safety Partnership as they are ideally placed to initiate a DHR and review panel due to their multi agency design. There is a procedure for the conduct of Domestic Homicide Reviews within County Durham, which includes processes for consent to be sought from family and friends for the sharing of relevant information for both the victim and the perpetrator/suspect.

The multi-agency Domestic Homicide Review Group, supported by the Home Office and HM Coroner Durham, endorsed the exchange of information between Durham Constabulary, Durham County Council's Children and Young People's Service and Adults and Health Services, General Practitioners and NHS. Materially relevant information and evidence to support, refuse and/or revoke firearm/shotgun licence(s) will be sought after a firearms/shotgun certificate holder has come to the attention of Durham Constabulary police due to:

a) Domestic abuse;
b) Any other safeguarding issues or concerns involving a certificate holder's partner and/or children;
c) Mental health; and,
d) Substance misuse.

5.8 Integrated Offender Management

Integrated Offender Management (IOM) approaches for those who offend in the community (both those on statutory supervision and those who are not) who present the highest risks to their communities, especially those short sentence offenders released from prison under no statutory supervision (including Priority and Prolific Offenders). It seeks to build on the work already done to 'prevent and deter' and 'catch and convict' those who offender by enhancing work done to 'rehabilitate and resettle' them. The strength of IOM is to manage those who offender in the community through multi-agency approaches, ensuring they are assisted in their rehabilitation through positive support, but also to ensure that deterrent, sanctions and enforcement measures are quickly activated for those people who offender that do no not comply.

IOM approaches draw on the resources and support of **all** relevant partners to supervise, resettle and rehabilitate people who offend. Multi-agency problem solving for identification, assessment, management and enforcement means that information sharing is a key part of the process. Information sharing takes place using a secure electronic site which members can access and update. Information on the electronic site is updated and shared at IOM Meetings. This negates the need to distribute papers or use hard copies.

5.9 Force Threat and Risk Assessment
As part of the Police Intelligence structures, on a monthly basis Officers of Durham County Council receive a copy of the Force Threat and Risk document via secure email from Durham Constabulary, which contains highly sensitive personal information regarding people who offend and victims.

Recipients of this document must manage its storage, retention and destruction in line with the principles set out in Appendix 3 of this protocol.

5.10 Channel and the Prevent Strategy
Implementing the Prevent strategy, which aims to stop people being drawn into terrorist and extremism related activity, involves statutory partners outside of this ISP. Referral processes are in place for personalised information to be shared with Durham Constabulary for assessment.

Where the police assess the individual as requiring a referral to the Channel Programme, Durham County Council has a statutory duty to ensure that a Panel is in place to assess the extent to which identified individuals are vulnerable to being drawn into terrorism and developing an appropriate support plan. The Channel Panel is dependent on the co-operation and co-ordinated activity of partners to ensure that those vulnerable to radicalisation receive support before they are exploited by those that would want them to embrace terrorism or engage in criminal terrorist related activity. Consent is required from the individual (and/or parent) to engage and receive a support package with the Channel Panel and for information to be shared between partner agencies. A confidentiality declaration is agreed to by all participating agencies attending the Channel Panel.

The multi-agency involvement in the Channel process is essential to ensure that vulnerable individuals have access to a wide range of support, from access to specific services provided by local authorities to diversionary activities. Information sharing is an essential part of the process to determine whether an individual requires support, and if so, what that should consist of.

Tension Monitoring Reports are used to gain an understanding of the impact that tensions and conflict may have on our local communities. There is significant value to be gained from Tension Monitoring across partner agencies.

5.11 Operation Encompass
Data on Domestic Abuse is shared between partners to build a picture of the prevalence and nature of domestic abuse in County Durham in respect of victims and perpetrators.

Operation Encompass provides a process for notifying a designated Key Adult within schools when a student was present in a household at the time when an incident of domestic abuse was recorded as having taken place. The school can then provide immediate appropriate level support to the child who may have been a victim or witness to the abuse, whilst in attendance at school.

5.12 Safe and Wellbeing Visits

Safe and Wellbeing Visits focus on vulnerable people and enhance prevention efforts through broadening the remit of fire safety visits to 'Make Every Contact Count' by identifying wider public health issues and referring people for support by partner organisations and the VCS. Lifestyle questionnaires are completed and referrals made with consent from the individual.

Data from safe and wellbeing visits can be utilised for service planning and prevention activity.

5.13 Serious Violence Duty

In order to collaborate effectively in the development of the Serious Violence Strategic Assessment and Strategy partnerships are expected to share data and intelligence. This should primarily consist of sharing aggregated and anonymised data but may also include data pertaining to individuals to inform the strategic, tactical and operational response to serious violence in the local area. For example, hospital data on knife injuries, the number of exclusions and truancies in local schools, police recorded crime, local crime data, anonymised prison data, areas of high social services interventions, and intelligence on threats such as county lines including the activity of serious organised crime gangs and on drugs markets. Data and information sharing between partnerships should be purposeful and the data used for the purposes of meeting the requirements of the duty to prevent and reduce serious violence.

6. Security

6.1 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). Article 32 of the UK GDPR requires organisations to put in place appropriate technical and organisational measures to ensure a level of security.

The ISO27001 provides a baseline for security arrangements, the Cyber Essentials Scheme has been developed by Government and industry to provide a clear statement of the basis controls all organisations should implement. Partners should ensure they have appropriate security in place and arrangements to monitor these.

A key issue, especially for electronic documentation, is the consistent use of encryption and secure information exchange. 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.

Information should not be processed on bring your own devices such as smartphones, tablets and laptops. Any staff who hold information on a portable device (e.g. laptop, USB stick) must ensure that the device is owned by their organisation, that it is password protected to comply with the standards of their own organisations procedures and that it uses the approved encryption software of their respective organisation.

Partners processing information under this agreement are responsible for ensuring that laptops, drives or removable electronic media containing personal information used for remote working are encrypted, and have Home Office approved levels of security. To comply with national guidance encryption should be at least 256 bit.

With respect to third party suppliers, recent Home Office guidance suggests that:

a) No unencrypted laptops or drives or removable electronic media containing personal information should be taken outside secure office premises.
b) No transferring of any protected personal information from Home Office approved systems to third party suppliers owned laptops, PCs, USB keys, external drives and any other electronic media is permitted.

6.2 Secure information sharing

Electronic exchange can be the most secure and auditable means of exchanging information provided this is done using suitably secure technology. Standard e-mail, even with encryption, is not generally sufficiently secure to protect personal information.

Personal information should only be exchanged electronically using a secure and encrypted messaging system such as the public service network or Transport Layer Security. Transport Layer Security (TLS)[4] 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
police.uk
nhs.net

DCC has a database of secure emails within its ICT Portal however this is only available internally by DCC staff. If in doubt then 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.**

6.3 Secure information storage and retention

Personal information must be held securely and managed effectively to ensure disposal once the specific purpose has been fulfilled. Partners should ensure that they follow the principles of secure storage and retention policies of their own organisations.

All records should be managed and reviewed to ensure that security is maintained and that nothing is retained longer than required for the specific purpose that led to its exchange. Paper records should be cross shredded and electronic records should be deleted in accordance with the agencies retention and destruction policies.

7. Indemnity

Home Office guidelines state that:

“As protocols are not legally-binding documents, it is wrong to assume that mention of indemnity clauses in any protocol would place all signatories beyond legal challenge, following a breach or disclosure of certain sensitive information.”

In line with this guidance an indemnity clause has not been included in this document and all issues should be resolved on a case by case basis.

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

8. Information breaches

Breaches of this protocol, complaints and incidents should be dealt with by utilising signatories' own organisations' established policies and procedures for incident management and complaints made in relation to any legislation in connection with information exchange.
At all events, parties 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/). All reportable incidents must be reported to the Information Commissioner's Office within 72 hours

Where data breach occurs that involves staff from any organisation who is a signatory to this agreement, it is essential that the details of the breach are reported to the Data Protection Officer at the organisation where the data breach occurred. This must be completed within 72 hours as it is a legal requirement. The Data Protection Officer from that organisation must communicate with the source agency as necessary and make the decision to notify the supervisory authority (ICO) of the data breach and lead a full investigation reporting the breach to all parties to share lessons learnt.

Each organisation should follow their own Incident Management or Data Breach process as required.

The source agency will share a summary incident investigation report with the relevant partners. The lessons learnt from that summary report should become the source of a review of the ISP to ensure mitigation can be implemented in case of similar incidents in future.

At all events, parties 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/). All reportable incidents must be reported to the Information Commissioner's Office within 72 hours

9. Right of Access (Subject Access) and other data subject rights

Each organisation will follow their own procedures when Data Subject Access Rights are requested. This includes access to their personal data, right to rectify, object and erase etc. Where there are implications for more than one organisations then this will be subject to consultation and discussion and agreement by those organisations.

If an agency 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.[5]

The principal exception is where a controller cannot comply with a request without disclosing information relating to a third party the Data Controller is not obliged to comply with the request unless

- The other individual has consented in writing to the disclosure of the information to the person making the request, or;
- It is reasonable in all the circumstances to comply with the request without the consent of the other individual.

[5] DPA 2018, Schedule 2, Part 1, Paragraph 2

All agencies need to co-operate speedily to ensure that requests are met within the one calendar month statutory time period set out in the Data Protection Act. The final decision to release the information rests with the agency that the information has been requested from in line with Data Protection regulations.

At all events, parties must follow the guidance of the Information Commissioner' Office on subject access and the other data subject rights (see https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/)

10. Business Intelligence

The Safe Durham Partnership will investigate the use of Power BI (Business Intelligence) in order to provide live time anonymised data to support the partnership's decision making processes.

11. Confidentiality Agreement

The information will only be used for a purpose other than the purpose for which it was obtained when that purpose is compatible with the original purpose, or there is consent, or there is a clear basis in law.[6]. It will be securely exchanged, stored and destroyed when no longer required. All agencies that are part of the information sharing process will when they sign this protocol, be bound by its terms.

12. Document Owner

This Information Sharing Protocol (ISP) is owned by the Safe Durham Partnership.

13. Commencement & Review

The commencement date of this protocol will be July 2021. This Agreement will be reviewed in 2023 or sooner if relevant developments or issues dictate.

[6] See https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/principles/purpose-limitation/

Review Team

The Review Team for this Agreement are;

Partner Organisation	Nominated Lead & role
Durham Constabulary	Leigh Davison, Information Manager
Durham County Council	Julie Bradbrook, Partnerships Team Manager
Durham County Council	Lawrence Serewicz, Information and Records Manager
County Durham & Darlington Fire & Rescue Service	Jon Bell, Information Services Manager
The Probation Service North East	Kay Nicolson, Head of Area for Durham and Darlington
County Durham & Darlington NHS Foundation Trust	Lisa Nattrass, Head of Data Security and Protection
Tees, Esk & Wear Valley NHS Foundation Trust	Louise Eastham, Head of Information Governance and Records Management
NHS County Durham CCG	Dr Ian Davidson, Director of Quality & Safety
HM Prison Durham	Phil Husband, Governor
East Durham Trust	Graham Easterlow, Chief Executive Officer

Appendix 1 Specific Datasets shared under the Police and Justice Act 2006 and other community safety legislation

Organisation	Datasets (for the area)
Police	1. Records on anti-social behaviour transport and public safety/welfare **incidents** recorded according to the National Incident Category List. Whatever information is recorded about the time, date, location and category of each incident must be disclosed. 2. **Crime records** recorded according to the Notifiable Offences list. Whatever information is recorded about the time, date, location and sub-category of each crime must be disclosed. 3. Records on individuals entering the **Channel** process (pre-criminal space), including name, gender, date of birth, address, support plan
Fire and Rescue	4. Records on **deliberate fires**, whether it was a deliberate primary fire (not in a vehicle), a deliberate secondary fire (not in a vehicle) or a deliberate fire in a vehicle. In addition, records on **incidents of violence against employees** and records of fires attended in dwellings where **no smoke alarm** was fitted. For all these records, whatever information is recorded about the time, date and location of the fire must be shared. 5. Records on **malicious false alarms**. Whatever information is recorded about the time and date of each call and the purported location of those alarms must be shared. 6. records on water safety incidents , time,date and location
Local Authority	7. Records on **road traffic collisions**. Whatever information is recorded about the time, date, location and the number of adults and children killed, seriously injured and slightly injured in each road traffic collision must be shared. 8. Records on **fixed term and permanent school exclusions**. Whatever information is held about the age and gender of the pupil, the name and address of the school from which they were excluded and the reasons for their exclusion must be shared. 9. Records of **racial incidents**. Whatever information is held about the time, date and location of each incident must be shared. 10. Records of **anti-social behaviour incidents** identified by the authority or reported by the public. Whatever information is held about the category, time, date and location of each incident must be shared. 11. Records on individuals in the **Channel** process including name, gender, date of birth, medical information, social care information, school/college information. 12. Records related to **housing** tenants where related to anti-social behaviour or selective licensing.
Health Clinical Commissioning Groups NHS Foundation Trusts GP records	13. Records on various categories of **hospital admissions**. The relevant admissions are those relating to the following blocks within the 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); and d) other entries where there is evidence of alcohol involvement determined by blood alcohol level (Y90) or evidence of alcohol involvement determined by level of intoxication (Y91).For each record, whatever information is held about the date of the admission, the sub-category of the admission and the outward part of the postcode (the first part of the postcode, before the space which separates it from the second part) of the patient's address must be shared. 14. Records of admissions to hospital in respect of **domestic abuse**. Whatever information is held about the date of the admission and the outward part of the postcode of the patient's address must be shared.

Organisation	Datasets (for the area)
	15. 12. Numbers of mental illness outpatient first attendances and persons receiving drug treatment. 16. Records of hospital admissions in relation to **serious violence**
Ambulance Service	1. 13. Records of **ambulance call outs** to crime and disorder incidents. Whatever information is held about the category, time, date and location of each ambulance call out must be shared.

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. Where an incident is recorded as a domestic incident, for example, 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. In the case of ambulance callouts, this should be the outward part of the postcode only.

Appendix 2 Authorised Signatory Form

COMMUNITY SAFETY INFORMATION SHARING PROTOCOL

Signatories to this agreement are;

Partner Organisation	Signatory Name & Title	Date
Durham Constabulary	**John Ward, Assistant Chief Constable**	**03/11/21**
Durham County Council	**Keith Forster** **Service Manager Operational Support (Caldicott Guardian)**	**31/10/21**
County Durham & Darlington Fire & Rescue Service	**Stuart Errington, Chief Fire Officer**	**06/08/21**
The Probation Service North East	**Kay Nicolson, Head of Area for Durham and Darlington**	**03/11/21**
County Durham & Darlington NHS Foundation Trust	**Jeremy Cundell, Executive Medical Director (Caldicott Guardian)**	**09/08/21**
Tees, Esk & Wear Valley NHS Foundation Trust	**Elizabeth Moody, Director of Nursing and Governance (Caldicott Guardian)**	**21/09/21**
NHS County Durham CCG	**Dr Ian Davidson, Director of Quality & Safety (Caldicott Guardian)**	**3/11/21**
HM Prison Durham	**Phil Husband, Governor**	**06/08/21**
East Durham Trust	**Graham Easterlow, Chief Executive Officer**	**10/08/21**

Information Lead Officers need to ensure that you have notified the Information Commissioners Office under the Data Protection Act to share information with other agencies for the purposes of the prevention or detection of crime and the apprehension or prosecution of offenders. This will need to be done through the Data Protection Officer or the individual in the organisation responsible for maintaining the Data Protection Notification.

On signing this form you are indicating that your Data Protection Notification has been checked and appropriately updated to reflect information sharing for this purpose.

Partner Organisation	Data Protection Register Entry Number
Durham Constabulary	Z4895895
Durham County Council	Z1808275
County Durham & Darlington Fire & Rescue Service	Z4757495
National Probation Service (Ministry of Justice)	Z5679958
Community Rehabilitation Company	Z2147102
County Durham & Darlington NHS Foundation Trust	Z1059396
Tees, Esk & Wear Valley NHS Foundation Trust	Z1387135
NHS County Durham Clinical Commissioning Group	ZA742736
HM Prison Durham	Z5679958
East Durham Trust	Z3506569

Appendix 3: Forcewide Threat & Risk Documents: Information Sharing Procedures

Information Sharing
The documents produced by Durham Constabulary contain sensitive personal information relating to victims and offenders. This includes vulnerable adults, children and young people. The document is produced to inform strategic tasking is also a vital document in identifying any risks relating to vulnerable individuals that can be brought to the attention of the appropriate agency.

The document is protectively marked as ‘restricted’ and will be shared, via secure e-mail, with appropriate Officers from Durham County Council (Community Safety, Community Protection, and Safeguarding).

Security
Hard copies of the documents must be kept in locked storage following the general principles for secure information exchange, storage and retention outlined in the ISP.

Appendix 4: The legal framework for sharing and exchanging information

1.1 Crime and Disorder Act (1998)

Section 115 of the Crime and Disorder Act 1998 provides a legal basis (not a statutory duty) for information sharing with relevant authorities where it is necessary for fulfilling duties contained in the Act. 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.[7] Section 17 of the Crime and Disorder Act 1998 also imposes a duty on responsible authorities to have due regard to the effect their work may have on crime and disorder, anti-social behaviour and substance misuse.

1.2 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.

1.3 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 1.

The Police and Justice Act 2006 also places a statutory duty on the strategy group of all crime and disorder reduction partnerships to prepare an information sharing protocol[8]. 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.

1.4 Other relevant Acts

Whilst the legislation highlighted in sections 4.1.1 to 4.1.3 above are the principle ones covering the exchange of information in respect of crime and disorder, there are a considerable number of other Acts that require or enable (subject to the wider law – see section 2 below) the sharing of information, including:

- Children Act 1989
- Children Act 2004
- Domestic Violence Crime and Victims Act 2004
- Anti-Social Behaviour Act 2003

---

[7] The Human Rights Act is now applied to the common law under the law relating tio the misuse of private information (see 2.2 and 2.3)

[8] Statutory Instrument 2007/1830 part 4 (1) and (2) require the drafting of an Information Sharing Protocol

- 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

2 Legislation governing the sharing of information

2.1 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. The lawful bases that are most likely to apply in the context of this protocol are; processing necessary for compliance with a legal obligation (Art 6.1(c)), and processing necessary for the performance of a public interest task or the exercise of official authority (Art 6.1(e)).

In addition, special category data can only be processed if there is an additional lawful basis under Article 9. The lawful bases that are most likely to apply in the context of this protocol are explicit consent (Art 9.2(a)) and processing necessary for reasons of substantial public interest (Art 9.2(g)).

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)[9] 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,[10] to protect the public against dishonesty or malpractice,[11] to comply with regulatory requirements relating to unlawful acts or dishonesty,[12] and to prevent fraud.[13] All of this processing is based on the 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.[14]

Moreover, the public interest must be 'substantial'.[15] That means the processing must be 'proportionate to the aim pursued, respect the essence of the right to data protection, and provide

[9] DPA 2018, section 11(2)
[10] DPA 2018, Schedule 1, Part 2, paragraph 10
[11] DPA 2018, Schedule 1, Part 2, paragraph 11
[12] DPA 2018, Schedule 1, Part 2, paragraph 12
[13] DPA 2018, Schedule 1, Part 2, paragraph 14
[14] DPA 2018, Schedule 1, Part 2, paragraphs 10,11,12 &14
[15] As above

suitable and specific measures to safeguard the fundamental rights and interests of the data subject'.[16]

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.

2.2 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. 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'.

2.3 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:

a) Is not already in the public domain.
b) Has a certain degree of sensitivity.
c) 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:

a) Where there is a legal compulsion to disclose.
b) Where there is an overriding duty to the public, this includes the need to prevent, detect and prosecute serious crime.
c) 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 is 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.

[16] GDPR, Art 9.2(g)

2.4 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 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:

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

2.5 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, which are not answered within the ISP Guidance Notes.

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 ISP that the originating authority is consulted before any release is made.