Home Office

Ministry of Justice

Data Sharing for the Criminal Justice System Guidance

October 2023

This publication is available at: Criminal Justice Board - GOV.UK (www.gov.uk)

Any enquiries regarding this publication should be sent to us at: CJS.DataImprovementProgramme@justice.gov.uk

Contents

Introduction and Structure of the Guidance

This **National Data Sharing Guidance** has been developed by the Home Office and Ministry of Justice in conjunction with other Government departments; key stakeholders including the Association of Police & Crime Commissioners (APCC), Association of Police and Crime Commissioners Chief Executives and the National Police Chiefs' Council (NPCC); and agencies across the Criminal Justice System (CJS). It is designed to encourage and enable those working in and with the CJS, including within Local Criminal Justice Boards, to share data - predominantly with the aim of performance improvement and strategic monitoring but also for operational effectiveness.

The majority of the data covered by the scope of this document will not contain personal data, as defined by the General Data Protection Regulation (GDPR). However, it is recognised that there will be circumstances where personal data will be shared. Whilst the main focus of this document is good practice sharing of non-personal data, it also covers data protection regulation and steps required to share personal data, as well as signposting to additional support where required.

Overview

More effective data sharing is essential to improving overall performance, criminal justice outcomes and operational delivery in the **Criminal Justice System** (CJS). Departments and agencies are looking to move to a more national and consistent approach to data sharing; improving the usability, timeliness and quality of data and ensuring it is handled appropriately within the relevant legislation and guidance. Key to this is removing barriers and facilitating all parties to share data better – including understanding the necessary skills, structures and enablers required.

This document provides nationally endorsed guidance to encourage and enable departments and agencies to share data with confidence, including through the forum of Local Criminal Justice Boards. It results directly from the recommendations in Part 2 of the Review of **Police and Crime Commissioners** (PCCs). The guidance has been coordinated with data workstreams of the **National Police Chief's Council (NPCC),** the **Crown Prosecution Service (CPS)** and the joint Home Office and Ministry of Justice **CJS Data Improvement Programme**. It should be read in conjunction with specific guidance to **Local Criminal Justice Boards** (LCJBs) supporting system-wide improvements. In particular, noting that the LCJB chair and members must respect policing, prosecutorial, and judicial independence and decision-making, as well as acknowledging that the LCJB chair cannot hold individual partners to account for their own agency's/organisation's performance.

The Police Reform and Social Responsibility Act 2011 set out in law the reciprocal duty on Police and Crime Commissioners (PCCs) and other Criminal Justice agencies to work together to provide an efficient and effective CJS for police force areas. This requires agencies to work together (while recognising their different roles and accountabilities).

PCCs therefore occupy an important place in the CJS, able to convene and co-ordinate partners on the collective mission to reduce crime, improve the efficiency and effectiveness of the CJS, and improve services to victims. As established local fora, the LCJBs are focal points for effective data sharing. In Wales, the Criminal Justice Board for Wales brings together the four Welsh LCJBs to share data, work together and tackle the systemic common CJS issues.

This guidance:

- Understands that the data landscape is fast-changing and technological innovations will enable ever greater data sharing and accessibility to data sets – and that this volume and complexity of data increases the need for clarity on how this should be handled;
- Provides clear national direction to those working in and with the CJS - particularly those on LCJBs - to encourage and enable them to share data with confidence;
- Predominantly focuses on performance data for system-wide monitoring and improvement purposes (but also addresses operational and personal data where they are relevant, informing users of data privacy regulations that must be considered);
- Sets out the practical considerations and tools needed to enable data sharing, understanding different data types and their characteristics to ensure the correct handling conditions are in place;
- Is not prescriptive about the specific data to be shared;
- Recognises the nuances of data sharing within the unique legislative and delivery context in Wales.

It has been developed by the Home Office and Ministry of Justice in consultation with the Association of Police and Crime Commissioners (APCC), Association of Police and Crime Commissioners Chief Executives (APACE), Attorney General's Office (AGO), College of Policing, the Crown Prosecution Service (CPS), Department of Health and Social Care (DHSC), His Majesty's Courts and Tribunals Service (HMCTS), His Majesty's Inspectorate of Constabulary and Fire & Rescue Services (HMICFRS), His Majesty's Prison and Probation Service (HMPPS), Information Commissioner's Office (ICO), the National Police Chiefs Council (NPCC) and the Welsh Government. A survey was also issued to all PCCs to understand their perspectives better. Over 20 responses were received, including a single response from all four Welsh PCCs, which included current example of good data sharing practice. These responses have been considered and examples of good practice have been included in the guidance. The Local Government Association has also reviewed the Guidance and are supportive of Local Government using it when interacting with the Criminal Justice System.

Embracing the guidance will drive greater consistency of data sharing – both in terms of the 'how' and the 'what' - and enable this to be done in a timely manner for the greatest impact on the CJS, victims and protecting the public. The guidance can be read as a whole or as standalone sections depending on the data sharing need to be met.

The guidance has three parts:

- **Part 1** looks at why the CJS needs to share data and some of the key obstacles in doing this,
- **Part 2** sets out the governance and key considerations necessary in advance of data sharing,
- **Part 3** focuses on the key questions and actions needed when seeking to request and / or share data.

The guidance fits into part of a larger landscape of regulatory requirements, pan-government policy, national and local guidance, and the process documents and technical controls that agencies deploy. It has been written to bring together relevant guidance and good practice to be of use to local practitioners and signposts where more detailed information or guidance can be obtained. It has also been written to provide flexibility for agencies to develop data sharing arrangements that work for them, while being consistent with national guidance.

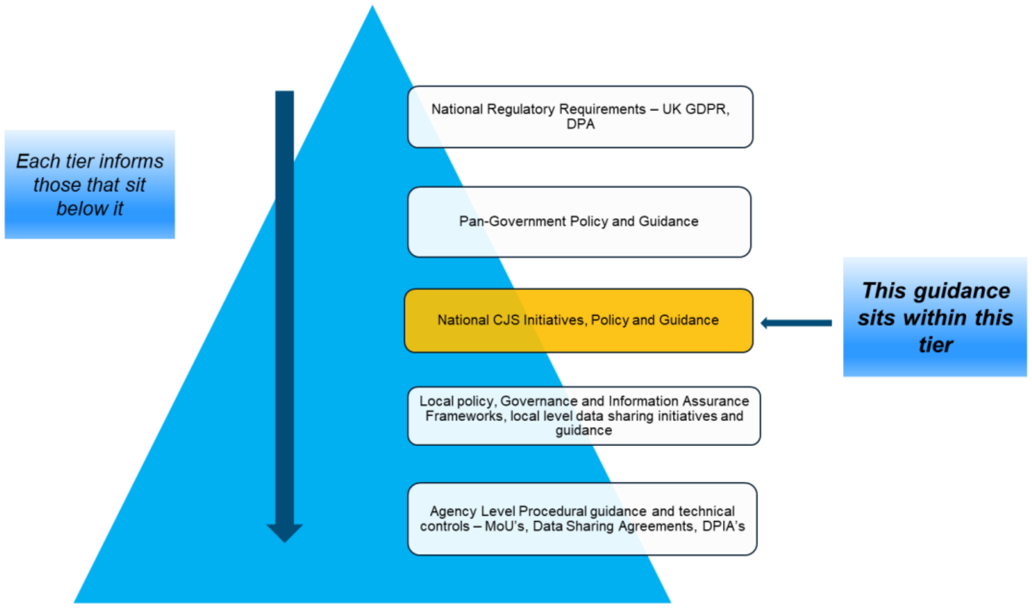

Each tier informs those that sit below it
National Regulatory Requirements – UK GDPR, DPA
Pan-Government Policy and Guidance
National CJS Initiatives, Policy and Guidance
Local policy, Governance and Information Assurance Frameworks, local level data sharing initiatives and guidance
Agency Level Procedural guidance and technical controls – MoU's, Data Sharing Agreements, DPIA's
This guidance sits within this tier

Fig 1: A diagram showing a hierarchy of documentation with National Regulatory requirements at the top, pan-government policy beneath than, this guidance document, local level policy and detailed local technical control documentation.

This guidance is accompanied by a **template Memorandum of Understanding** (MoU) that can be used to facilitate data sharing across the CJS at a local level when an existing agreement is not already in place.

<u>NOTE:</u> The guidance will not outline which data should be shared. It is intended to provide information relating to considerations and tools that ensure data sharing is carried out in the correct way, and to affirm the intention for organisations across the Criminal Justice System to share data when possible. Please refer to local policy, data sharing initiatives and guidance to determine specific resources that can be shared.

PART 1: The Context of Data Sharing in the Criminal Justice System

This section sets out the context of the Guidance, its background and focus, and specific strategic aspects of data sharing that are particularly relevant for those who work in and with the CJS.

1 Purpose and Scope

1.1 Purpose

This guidance is designed to facilitate better data sharing both within and with the CJS for improved efficiency and effectiveness. Bodies across the CJS agree that data sharing is positive and to be encouraged, while recognising that it must be done lawfully, safely, proportionately and appropriately. By following this guidance those working in and with the CJS will be better able to ensure that information provided is shared correctly is accurate and timely, and used for the purpose for which it was intended. It is important that all those working in or with the CJS operate from a shared and consistent view of data to have an agreed understanding of what is happening, what needs attention and what action should be taken. Significant steps have already been taken towards this with the creation of the CJS Delivery Data Dashboard[1] and Digital Crime and Performance Pack (DCPP) and this guidance is designed to continue to support such initiatives, as well as enable better data sharing locally.

EXAMPLE: *As an example of an area sharing local data alongside national data, a Combined Authority creates and maintains a range of interactive secure access online dashboards including a range of data from criminal justice, health, and victims' services. These dashboards are updated on a regular basis and available to local agencies and partners supported by a long-standing data processing agreement.*

1.2 Scope – Data Types

The guidance is predominantly focused on encouraging and enabling the sharing of **performance and strategic data at a local level**, and does not cover Data Sharing for law enforcement purposes in detail. For sharing data relating to law enforcement purposes as defined under DPA 2018 Part 3, namely for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security, you must follow well established processes and comply with the statutory duties.

[1] Home - CJS Dashboard (justice.gov.uk)

The guidance is written for all agencies within and who work with the CJS, particularly PCCs and those agencies that sit on LCJBs, to enable them to share data in a more consistent, timely and focused way to deliver performance improvement collaboratively across the end-to-end CJS at a local level. Data shared via PCCs and LCJBs can be used to understand national, regional and (particularly) local demand and trends to shape future policy, identify specific challenges, and design, deliver and monitor the effectiveness of strategies and operational performance improvement.

More widely this guidance and the associated Memorandum of Understanding (MoU) template can also support criminal justice and other agencies to understand and enable how best to share data for crime reduction purposes and public safety. Such data sharing between agencies may enable swifter, more targeted action to be taken to prevent crime. Combining key data sets can enable better and more timely decision making by enabling agencies to build a full picture of drivers for issues and may also help to identify where funding could be directed to help deliver community safety/ crime prevention initiatives.

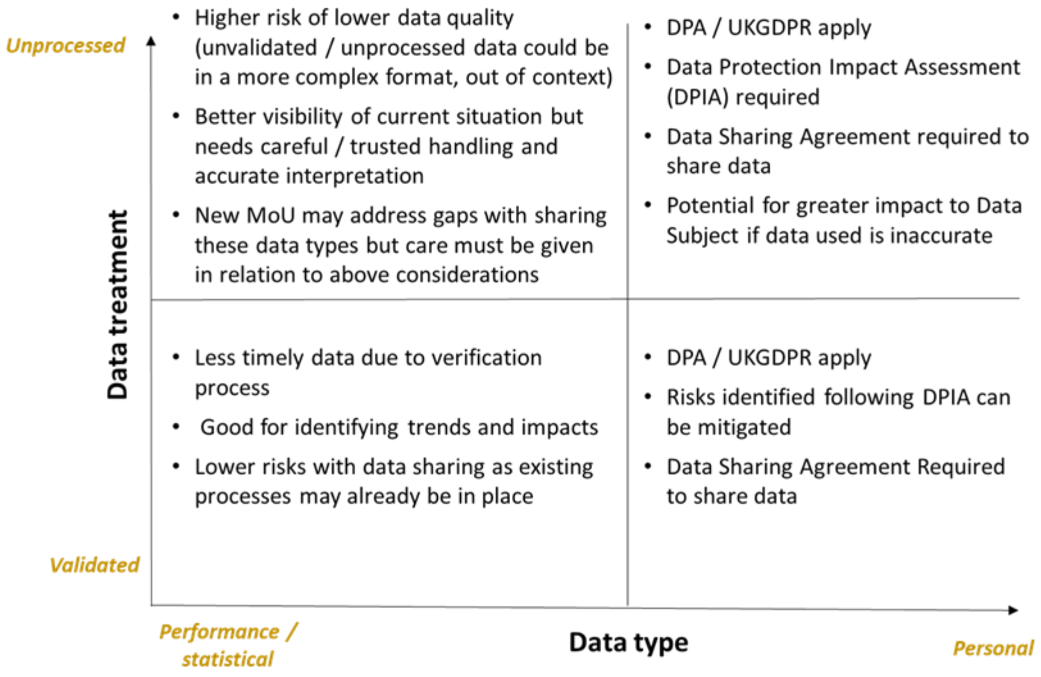
***NOTE:* Due to the nature of data collected across the CJS there will be times when data for performance monitoring contains aggregated, non-personal data where the underlying data source used contains personal data. It is important to have a clear understanding of the end-to-end sharing process to determine whether personal data falls into the scope of the data sharing and therefore is subject to data protection legislation.**

While not the main focus of this guidance, it is recognised that **personal data** may need to be handled at different times in support of performance and strategic work, such as dip sampling of compliance with the Victims Code of Practice, or deeper dives into understanding performance or crime patterns. As such, this document highlights the additional steps needed in these situations.

A key dimension to data sharing is the **timeliness of the data**. More timely data can provide a better up-to-date picture of performance and enable better cross-agency decision-making. However, it may be less validated and therefore in need of greater care and analysis when drawing conclusions. This guidance encourages agencies to share performance data they hold with their partners, and to address upfront any issues relating to how analysis is undertaken and controls over publication so that such data can be shared confidently.

It is essential that there is trust and confidence across all those working in and with the CJS that data is handled sensitively and by those who can understand it best. To engender such a culture of trust, the body requesting data should work with the provider to analyse the data, to take into consideration any data quality issues, as well as the wider contextual picture underpinning the data.

The diagram below is a simple illustration of different data that may be shared and is not exhaustive. There can always be exceptions. For example, there may be instances where personal data could be statistical, and data may sit between completely unprocessed and fully validated.



- Higher risk of lower data quality (unvalidated / unprocessed data could be in a more complex format, out of context)
- Better visibility of current situation but needs careful / trusted handling and accurate interpretation
- New MoU may address gaps with sharing these data types but care must be given in relation to above considerations

- DPA / UKGDPR apply
- Data Protection Impact Assessment (DPIA) required
- Data Sharing Agreement required to share data
- Potential for greater impact to Data Subject if data used is inaccurate

- Less timely data due to verification process
- Good for identifying trends and impacts
- Lower risks with data sharing as existing processes may already be in place

- DPA / UKGDPR apply
- Risks identified following DPIA can be mitigated
- Data Sharing Agreement Required to share data

Fig 2: A diagram showing risk levels increasing with unprocessed personal data and decreasing with validated performance or statistical data.

1.3 Scope – Organisations

This guidance is a tool to be used by anyone working in or with the CJS but is particularly relevant to:

- **PCCs** as a convening role;
- **LCJBs and the Criminal Justice Board for Wales** as focal points for effective data sharing;
- **Operational, local CJS agencies** – the police and wider law enforcement agencies, HM Courts & Tribunals Service (HMCTS), HM Prison and Probation Service (HMPPS) and the Youth Justice Board (YJB) who can share data to improve CJS outcomes;
- **Other public services** that have a key role to play in supporting and working with the CJS in crime reduction and public safety, particularly those focused on healthcare, education, and local government;
- **Government departments**– including the Home Office, the Ministry of Justice (MoJ), the Attorney General's Office (AGO), the Crown Prosecution Service (CPS), and the Department of Health and Social Care (DHSC);
- **Welsh Government;**
- **National co-ordinating bodies** – APCC and NPCC, who can set the framework for effective data sharing, support national and local data sharing initiatives, and share good practice

EXAMPLE: *As an example of data sharing from other local public services, one local authority provides a Violence Reduction Unit with education data regarding exclusions, violence in schools and safeguarding data under an Information Sharing Agreement to understand trends and assess the effectiveness of interventions.*

1.4 Scope – Usage

This guidance recognises that there are already many examples of local data sharing initiatives, often created for specific purposes. It does not seek to replace these but rather looks to put in place consistent guidance to enable greater data sharing at the local level. Where there is already approved guidance relating to a specific data sharing initiative this should persist provided it is consistent with this guidance. Where none exists or wider data sharing is needed, this document (and accompanying template MoU) provides the information necessary to make informed decisions on data sharing.

The MoU sets out data sharing requirements between parties and should be completed and signed before data sharing takes place. If data sharing requirement includes the use of personal data, Data Protection Impact Assessment (DPIA) screening should be carried out to determine whether a full DPIA is required. This will be done in conjunction with your data privacy team or DPO.

2 Understanding Data Sharing for the Criminal Justice System

For the CJS to function effectively data needs to be shared consistently and in a timely manner to ensure a common view of the challenges and opportunities. As CJS data becomes larger, more available and insightful, the need and opportunity for effective data sharing becomes more important to realise the benefit from the available data, ensure decision making is data driven and support all parties to work proactively and collaboratively to improve outcomes.

2.1 Why We Share Data

Data sharing across the CJS and with other partners at local level can deliver significant value. It is important to share data to:

- Ensure a better understanding of the local criminal justice picture and which levers to pull / interventions to make to improve the effectiveness of the CJS;
- Have a system-wide view of performance – understand the end-to-end journey and experience of those who pass through the system;
- Identify and address gaps in service delivery;
- Improve the running and effectiveness of LCJBs;
- Engage non-CJS partners effectively in sharing data that helps support wider crime reduction and community safety objectives, and supporting policy development;
- Reducing un-met need – i.e., identifying where someone is not picked up in a certain dataset that suggests they are not receiving a service that a frontline practitioner thinks they should be – they can then make the referral (GDPR considerations will apply);
- Supporting better coordination between services and agencies to manage someone's case and reduce the likelihood of something critical being missed, e.g., an offender's health condition (GDPR considerations will apply);
- Reduce the number of times a service user must repeat information to different agencies.

EXAMPLE: *In one CJS area, an analyst group has been created to explore specific issues and support the LCJB. These are experts in the data for their own CJ organisation so they understand what is available and how it can be used. They operate within an MoU for data sharing.*

2.2 Challenges This Guidance Aims to Address

The desire to improve data sharing in the CJS is long-standing and considerable progress has been made in key areas. The purpose of this guidance is to build on this and drive consistency to enable a culture of 'data sharing'. From engagement with Government departments, criminal justice agencies, PCCs and others a range of obstacles to data sharing have been identified, which this guidance seeks to address constructively, including:

- **Strategic considerations / considerations of principles** such as:
    - Misapplication of legislative constraints;
    - Perceived lack of national endorsement of data sharing;
    - A lack of aligned incentives between the parties sharing data;
    - Overly complicated, opaque and unwieldy governance processes to access data;
    - Reputational concerns and trust – particularly regarding data entering the public domain;
    - Confidence in how the data will be used / analysed / interpreted;
    - Misunderstandings re local duties and responsibilities (including of PCCs and LCJBs);
    - Inconsistencies and lack of baselining of what is possible;
    - Requests for more timely data and the associated analysis and handling requirements;
    - Risks of individuals being identifiable from performance data dependent on volume / sample size.
- **Tactical / practical considerations** such as:
    - Inconsistencies / differences in how things are counted / comparable data;
    - Inconsistencies around platforms and tooling;
    - Poor data quality;
    - Lack of unique identifiers that are common across systems;
    - Lack of searchable metadata or cross-government data catalogues, meaning data discovery is poor;
    - Clarity on roles, responsibilities and where to go for data in organisations;
    - Implications of novel combinations of data sets to solve problems;
    - An over-reliance on good relationships for effective data sharing;
    - Lack of agreements to share data between major departments and agencies;
    - Practical challenges in recording the data needed – especially if not a 'native' need of the providing organisation.

This guidance has been created to contribute towards tackling these obstacles and allow quick access to the process for data sharing within the CJS and with other partners. The remainder of the document provides information on underpinning considerations when preparing for data sharing, and the practical steps to take when actively seeking to share data with partners.

Part 2: What to Consider When Sharing Data

Having established the ambition for greater data sharing across the CJS in Part 1, this section sets out some of the conditions and considerations to address in preparation for data sharing. It includes key principles, legislation and other requirements, as well as key areas of focus to be 'data sharing ready'. Each CJS agency has its own policies and procedures related to data sharing, and these will also need to be considered when sharing data locally.

3 Data Sharing Principles

3.1 Data Sharing Governance Framework –Data Sharing Principles

The Government published the **Data Sharing Governance Framework** in May 2022[2]. This sets out five principles to follow to make data sharing more efficient: Commit to **leadership and accountability** for data sharing – using / reusing data should be a strategic priority (including making data accessible and accessing data from elsewhere). Senior leaders need to understand the strategic importance of data sharing, make data sharing a strategic priority and create a culture that supports those working to solve data sharing problems.

2. Make it **easy to start data sharing –** organisations can make data sharing more efficient by making it easier for others to start a conversation about it, from identifying contacts to transparency on what information is needed from data requesters.
3. **Maximise the value** of the data you hold – data sharing is made slower and more difficult when there is a lack of transparency about what data exists and how it can be accessed. It is easier to realise the value of data the more that is known about the data held and who is responsible for it. This also makes it easier for others to understand its value and start conversations about it.
4. Support **responsible data sharing** – sharing data (particularly personal data) can be seen as a high-risk activity, but this should not discourage sharing where there are good reasons to do so, and in cases of personal data, where there is a legal basis. Consideration should be given to data protection law and national guidance[3] to make sure that data is shared responsibly. Some sensitive data has special legal protections which may restrict sharing, such as data held by healthcare organisations. Non-personal data can be shared with more flexibility if an organisation has different plans to share different kinds of data in different ways.
5. Make data **findable, accessible, interoperable, and reusable** – using common data standards is very important here. Data standards help people to agree and document the content, context and meaning of data. This includes how it is represented, recorded, stored, and accessed. Better findability, accessibility, interoperability and reusability means everybody can get more value from shared data and that the data can be shared and used more quickly.

[2] Data Sharing Governance Framework - GOV.UK (www.gov.uk)

[3] Data Protection Act 2018, ICO's data sharing code of practice, government Data Ethics Framework, the NCSC's cyber security guidance

3.2 Local CJS Data Sharing Principles

Building on the principles above and with the aim of data sharing being a key enabler of efficiency and effectiveness in the CJS, the following principles have been developed for local CJS data sharing:

1. Provision of **accurate, timely and consistent data** to:
    a. Enable performance monitoring and improvement of the end-to-end CJS, particularly for victim, witness, and offender journeys;
    b. Enable improvements to CJS outcomes for victims;
    c. Enable statutory duties to be fulfilled;
    d. Support agencies in delivering their operational functions and responsibilities.

    Handling personal data, including special category data, will require additional care in line with legislative, policy and other relevant constraints (see section 5 below).

2. Data should only be shared under **clear and approved agreements**, and with those most appropriate to receive it.
3. Shared data should only be **used for its intended / approved purpose** and not shared more widely / for other purposes without the express agreement of the agency that owns the data.
4. Where there is a request for data as part of an analytical project, there needs to be joint agreement that the proposed analytical methodology is sound.
5. Requests for data should be **justified, appropriate, proportionate, auditable (traceable) and necessary and should be limited to the minimum data required to achieve the stated purpose(s)**. Where requests come from LCJB members requests should be linked to the given LCJB's business plan where possible, and respect the independence of agencies they are requesting data from.
6. **Retention and deletion policies** for shared data should be clear and agreed in advance.

4 National Regulatory and Policy Requirements

National regulatory and policy requirements, such as data privacy regulation and pan-government policies on information security, need to inform all local data sharing decisions.

The approach to sharing data will depend upon the nature of the data being shared. More detail on how to consider this is provided in Part 3 but a summary view is provided below.

4.1 Regulation and Legislation

The major regulatory requirements are the UK General Data Protection Regulation (UK GDPR) and Data Protection Act 2018 (DPA 2018). Engagement with stakeholders during the production of this guidance highlighted that these were often cited to block CJS related data sharing.

While these requirements are important, it should be noted that they address the handling of personal data. This guidance predominantly focuses on CJS sharing data for performance improvement and strategic monitoring. If the data to be shared cannot be used to directly or indirectly identify an individual or cannot be combined with other data to identify individuals, the UK GDPR/ DPA 2018 are NOT applicable.

There will however be occasions where sharing personal data may be necessary, such as to undertake dip sampling into compliance, to do deeper dives into performance patterns, or combine different data sets to produce a full understanding of crime trends. In such situations, the data should always be anonymised / pseudonymised wherever possible and additional steps taken to safeguard data.

Anonymisation *is information that does not relate to an individual and is therefore no longer 'personal data' and is not subject to the obligations of the UK GDPR. You must carefully assess each case individually based on the specific circumstances of data sharing to help you decide the effectiveness of an anonymisation technique – this should always be carried out in conjunction with your data privacy team or DPO.*

Pseudonymisation *of data is the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information. Pseudonymisation is considered a control to minimise risk to personal information but will not eliminate it as it may still be possible to identify individuals. For this reason,* ***pseudonymised data IS subject to personal data privacy legislation.***

There must be a defined **Lawful Basis** for the sharing of personal data (under UK GDPR, lawful bases for processing are set out at articles 6 and 9 - with reference also to Schedule 1 to the DPA 2018). Further detail is provided in Annex A1 of this guidance.

Should there be any doubt about data anonymisation, or whether there is a risk from collation of data, the agencies / individuals involved should engage their data privacy team / Data Protection Officer.

NOTE: ***Victim Code of Practice monitoring and dip sampling may contain personal data or pseudonymised data that falls under data protection legislation and so data sharing for this purpose should follow enhanced controls.***

Where personal data does need to be shared the national regulatory and policy requirements apply and agencies need to know when / how to use them. A summary of regulations and guidance relating to personal data can be found in Annex A1. In addition, the ICO has a Data Sharing Code of Practice, referenced here Data sharing: a code of practice | ICO

In Wales, the Wales Accord on the Sharing of Personal Information (WASPI) was established across health and social care, local authorities, emergency services, education providers and other organisations to help them meet data protection responsibilities. WASPI has proven to be an invaluable tool in the continued drive of collaboration and standardisation between public services and the associated requirements for effective, safe, and legal sharing of personal information.

EXAMPLE: *In one area, CPS shared case numbers of instances where the case had ended due to victim and witness attrition; this enabled the LCJB and other agencies involved in the process to examine these cases to find out why they failed and to bring about improvements.*

4.2 Freedom of Information Act (FoIA)

The Act covers all recorded information held by a public authority. It is not limited to official documents and it covers, for example, drafts, emails, notes, recordings of telephone conversations and CCTV recordings. The Act includes some specific requirements to do with datasets. For these purposes, a dataset is collection of factual, raw data that is gathered as part of providing services and delivering functions as a public authority, and that is held in electronic form.

Information can be found here: Freedom of Information Act 2000 (legislation.gov.uk)

An MoU or Data Sharing agreement will set out requirements for Freedom of Information (FoIA) requests. Where an MoU is not required but the request is for shared data, the agency receiving the request **must notify the other to allow it the opportunity to make representations on the potential impact of disclosure and issue a formal response following its internal procedures for responding to FoIA requests, within the statutory timescales.**

How does the Freedom of Information Act affect data protection?

The Freedom of Information Act comes under the heading of information rights and is regulated by the ICO. When a person makes a request for their own information, this is a data protection subject access request. However, members of the public often wrongly think it is the Freedom of Information Act that gives them the right to their personal information, so there may need to be clarity on this when responding to such a request.

When someone makes a request for information that includes someone else's personal data, there is a requirement to carefully balance the case for transparency and openness under the Freedom of Information Act against the data subject's right to privacy under the data protection legislation. A decision will need to be made on whether the information can be released without infringing the UK GDPR data protection principles.

More information can be found on the ICO website: What is the Freedom of Information Act? | ICO

4.3 National Government Policy and Guidance

There are several National, Pan-Government policy and guidance documents and sources related to data that also need to be taken into account. Agencies will have governance in place to ensure that these are being followed and the adoption of the guidance should be proportionate to the type of information being handled:

- Policies Relevant to Data Sharing:
  - Data Sharing Governance Framework Data Sharing Governance Framework - GOV.UK (www.gov.uk)
  - The Security Policy Framework Security policy framework: protecting government assets - GOV.UK (www.gov.uk)
- Further Information on data security best practice as set out by the Government that impacts data sharing requirements can be found below. These give a wider picture of information security across UK Government, rather than being direct links to specific data sharing requirements and are not required in order to fulfil the obligations in this guidance.
  - National Protective Security Authority (NPSA) formerly CPNI National Protective Security Authority | NPSA
  - The National Cyber Security Centre (NCSC) National Cyber Security Centre - NCSC.GOV.UK

4.4 Considerations Relating to Sharing of Health Data

Health data can be used in conjunction with other data sets for performance purposes and to improve outcomes for people, communities and the teams who serve them.

Due it its sensitive nature, the potential impacts to individuals if confidential patient information is shared, and the public interest served by maintaining public trust in the confidentiality of services provided by health and care organisations there are some additional considerations around sharing this type of data:

- Health data that has been anonymised can be shared.
- Under the common law duty of confidentiality, confidential patient information that identifies individuals either directly or indirectly can only be shared if there is a court order or legislation requiring disclosure in place, or the valid, informed consent of the individual has been gained to share the data, or if there is an overriding public interest justification for disclosure. There must also be a legal basis for processing under UKGDPR.

If an organisation concludes there is a need to access confidential patient information for direct law enforcement purposes, they should continue to use already established local mechanisms (such as a standardised DP9/DP7 form) and guidance on the legal and ethical considerations of requesting the data.

A guidance document, NHS Code of Practice Supplementary Guidance on Public Interest Disclosures is accessible via:https://www.gov.uk/government/publications/confidentiality-nhs-code-of-practice

If an organisation wishes to access anonymised or pseudonymised “trend” style data from health bodies (for example occurrences of stab wounds over a given period), LCJBs and PCCs should establish contacts with their local Integrated Care Board(s)(ICB).

The Integrated Care Systems (ICS) were established in The Health and Social Care Act 2022 to enable a move toward closer working between organisations within the health and care system. Within each ICS there is an ICB which, among their other duties, will facilitate integration between local NHS organisations in their area.

It is unlikely the ICB will be the data controller of any data sought, however building a relationship with the ICB can help facilitate and manage requests to health data controllers in their area of responsibility.

5 Data Sharing Governance

Having the correct governance in place is key to ensuring effective and compliant data sharing regardless of the precise nature of that data. Each organisation will have its own Information Governance and this section sets out the areas within this to be considered in relation to data sharing. Applying and regularly reviewing the application of this guidance will enhance an organisation’s readiness for data sharing.

Local Criminal Justice Boards are encouraged to regularly review current and new data sharing needs and maintain up to date information on sharing that is in place, and respective roles and responsibilities.

5.1 Data Sharing Roles and Responsibilities

Information assurance and data privacy roles cover responsibilities to share data efficiently and effectively. The list of roles below is not exhaustive (and they may have different names in different organisations) but highlights those that are typically engaged with as part of data sharing requests. These are defined roles and individuals will have received training and responsibilities of the role. By understanding these roles and who holds them, the process of making data sharing requests can be accelerated. To make data sharing easier, it is encouraged to identify roles locally in advance so they can be involved as early as possible in data sharing discussions.

Role	Responsibility
Senior Information Risk Officer (**SIRO**)	A SIRO has responsibility for managing information risk. The SIRO will advise senior management on information risks.
Data Protection Officer (**DPO**)	The DPO is responsible for providing oversight and advice on Data Privacy, including ensuring Memorandum of Understanding or Data Processing Agreements provide appropriate coverage.
Data Protection Practitioners	Across some agencies this role is in addition to the DPO. They provide support and advice to the business.
Chief Data Officer (**CDO**)	CDO's are responsible for managing data and analytics operations and increasing operational efficiency.
Information Management Key Points of Contact	Different organisations may have different titles for this role (e.g. Data Steward, Data Custodian). The role is an enabling function to support the business area, and general data management and data sharing questions can be addressed.
Information Asset Owner (**IAO**)	IAOs, sometimes known as Data Owners, are the individuals that take responsibility and ownership of a data set. In some organisations an IAO has the equivalent accountability of a SIRO. They are responsible for the update of Records of Processing Activities (RoPA).
Data access and acquisition teams	In larger departments, these teams are often the first point of contact for data sharing.

When sharing data:

- Identify what data needs to be shared to achieve your aim, make sure you only share/ request the data that you need to;
- Ensure data subject rights are considered as part of your proposal if personal data will be required *(Refer to Annex A of this guidance for further detail);*
- Determine who fills these roles to accelerate making / receiving data sharing requests where formal sign-off or approval may be needed;
- Ensure any other local or national data sharing roles and responsibilities are clear - knowing who records requests, who accepts or manages risks, and who can sign DSAs or make sharing approvals and who needs access to the data;
- When making / receiving a data sharing request where an MoU or DSA is required, anyone other than the designated role **must not** sign on behalf of one of these roles. By signing an individual takes responsibility for risks and issues and will be held accountable as the signatory should an information security breach occur;
- For ad-hoc requests at practitioner level sign off by a senior responsible individual would not usually be required;

- Be clear upfront on any specific data sharing requirements, such as handling instructions, considerations that need to be taken into account when undertaking analysis (such as joint analysis, or joint sign-off of findings) and restrictions surrounding publication or freedom of information requests;
- Have access to the necessary secure platforms for data sharing and the dashboards and systems needed.

NOTE: ***By having agreements in place for regular access to data it is possible to obtain the information required without repeated requests and creating additional workload.***

5.2 Data Sharing Documentation

Data sharing should always be documented. A template MoU accompanies this guidance to facilitate systematic, or regular data sharing locally. Although an MoU is not a legal requirement for sharing non personal data, it is good practice. An MoU is appropriate for sharing of personal data where the other party conforms to the same government requirements for security, and a Data Sharing Agreement (DSA) is appropriate where this is not the case. In Wales, templates for the

sharing of personal data have been agreed by the WASPI Management Board and should be used by any organisation signed up as a WASPI Accord signatory. The templates can be found via: Templates and guidance - Welsh Accord on Sharing of Personal Information (gov.wales). Information Sharing Protocols created via the WASPI framework will be subject to the quality assurance processes.

In all cases of sharing personal data, DPIA screening should be carried out, and you will also need to complete and publish a privacy notice. DPO or data privacy contacts can assist with this.

NOTE: ***The terms 'MoU' and 'DSA' can be used interchangeably across the CJS. Some organisations may also title these documents as an 'Information Sharing Agreement' (ISA). The key is that the content of the document meets the requirements for the data sharing.***

When developing data sharing documentation, bear in mind:

- The documents provide a framework for the sharing and use of data, to ensure transparency and assurance;
- Once in place, data can be freely shared within the scope identified in the document. Any required changes should be outlined in an updated MoU;
- Ad-hoc requests for different data sets not included in the documentation will need to be addressed separately;
- The documents must be subject to regular review (at least annually) and in the event a change or adjustment is required to the data sharing arrangement.

MoU	**DSA**
An MoU is an agreement between two or more parties that sets out a common agreement for data sharing requirements. The content of an MoU will differ depending on requirements, but will commonly include the following: • Parties to the agreement (controllers involved) • Other organisations involved • Purpose • Data to be shared • Information governance When making or receiving a data sharing request, the content of the MoU should match the requirements for handling the data.	A DSA is required when your data sharing contains personal information, as defined by the ICO. It will commonly include the following sections: • Parties to the agreement (controllers involved) • Other organisations involved • Purpose • Data to be shared • Information governance • Lawful basis • Lawful basis and legitimising conditions (for special category personal data) • Information rights Article I. Further information on DSAs can be found on the ICO website: Data sharing agreements | ICO
DSA Terms may also be incorporated into an MoU as needed	
In many cases once the DSA/MoU is complete organisations will require that a Data Movement Form is completed. The form documents how, when and where the data has been transferred.	

5.3 Equality Impact Assessments

Public sector organisations have a legal duty under the Equality Act 2010 to give due regard to certain relevant considerations, including eliminating conduct which is unlawful under the Act.

Equality Impact assessments should be done when a new data sharing process is begun, or when an existing one is reviewed. The Equality Act remains relevant when handling information for FOIA purposes.

5.4 Incident Management

Even with controls and procedures in place mistakes can happen. It is important that any potential or actual incident is flagged as soon as it is known, so that steps can be taken to minimise the risk. Some examples of potential incidents are:

- Data with a security classification being sent to a personal email address (Gmail, Hotmail etc);
- Emailing a file in error or to the wrong individual;
- Accidental disclosure;
- Personal Data not fully removed from a data set before sharing;
- A user logs on to a system with their credentials and allows another individual that has not been authorised to access the system;
- A user downloads data from a system onto a laptop without approval;
- A data set becoming corrupted and unavailable;
- The integrity of a data set being compromised.

Actions and escalation routes in light of an incident should be set out in the MoU, such as to notify the incident management team/ point of contact in order that remedial action can be taken.

Typical responsibilities in light of an incident include:

- Informing the relevant security team immediately of a potential incident is identified in line with your departments reporting requirements for both internal security purposes and compliance with Data Protection legislation;
- Attempting to secure and/or rectify the data should there be accidental disclosure of information (for example, sending an email to the incorrect address).

For Personal Data Breaches

If a breach is likely to result in high risk to rights and freedoms of individuals, those concerned must be informed without undue delay of the breach (including likely consequences and measures taken in response) (DPA 2018 s. 68).

If a breach is not unlikely to result in (any level of) risk to rights and freedoms, the ICO must be notified without undue delay, and within 72 hours of becoming aware where feasible (s. 67 DPA 2018).

5.5 Data Retention and Disposal

Agencies will have a data retention schedule outlining a retention policy for different data types. Detail around data retention where it is likely to fall outside of standard organisational retention policy should be clarified in the supporting agreement (MoU/DSA) and agreed by all parties, including how this will be managed/facilitated.

In relation to data sharing:

- When making or receiving a data sharing request, it must be set out how long the data will be retained for, and when and how it will be disposed of (or deleted);

- If the receiving controller is using data for legitimate purposes as agreed in the data share, then their own retention policy will be appropriate and normal review at the end of that applies, unless a restriction has been placed upon the retention at the outset or the joint purpose dictates the retention period. Under these circumstances a request can be made at the end of a retention period to renew the retention and therefore retain the data for longer, but this needs to be recorded and agreed by all parties – a business purpose must be identified for this. The Record of Processing Activities (RoPA) sets this out in detail – these are managed by IAOs/ Data Owners.

5.6 Government Security Classifications and Data Sharing

Data in scope of this guidance is likely to be OFFICIAL / OFFICIAL-SENSITIVE.

Local Information Security teams will be able to provide support relating to technical and organisational (procedural) measures for material subject to a security classification. Some good practice measures when dealing with classified data include:

- Ensure data is handled in line with requirements for the classification;
- Ensure that the recipients of data sets have appropriate clearance to access it (BPSS, SC, DV). Note that staff within Police and Crime Commissioner’s offices are vetted and can access data appropriate to their clearance level;
- Data may be de-classified once it has gone through analysis, anonymisation and publication, but this must be done in line with agreed procedures;
- Do not lower the security classification of documents or data sets to facilitate data sharing without analysis / sanitising of the data set and gaining necessary approvals from the Information Asset Owner.

6 Data Quality & Definitions

Good quality data is key to efficient data sharing. Poor data quality was a repeated concern from stakeholders engaged in the production of this guidance - sending / receiving data that is not of the right quality or does not have the scope of the data clearly defined can impact its use. Impacts of providing poor quality data could include:

- Statistical or performance data not giving an accurate reflection of what is happening, meaning opportunities to provide support are missed or agencies are unnecessarily scrutinised;
- Data analysts take extra time checking / revising data, risking it being out of date when used to inform work or when published.

The desire to improve data quality before it is shared needs to be balanced against the value of sharing timely data between agencies. It is important to be clear on the quality of the data being shared and consideration of whether it is of sufficient quality for it to meet the objective for which it is being shared. It is also important to be clear on usage and publication of such data.

***<u>NOTE:</u>* A use-case that involves the data being used to make a decision about an individual is likely to require highly accurate and timely data, whereas a use-case that involves an analysis of a large aggregated longitudinal set of data may have higher tolerance for errors or false positives in records, both because the stakes of the decision are lower in the short term and individual errors are less consequential if the overarching trend is correct.**

Similarly, data used to make day to day performance decisions is likely going to need to be timelier than data used to support research and policy development.

Consideration of the following will minimise the risk of sharing data that is not of good quality or helpful for the purpose it was intended for:

Data consideration	Guidance
Data Format	Agencies collect and record data in different ways for their own purposes. This can cause discrepancies when analysing data sets from differing sources. In addition, it is recognised that there is sometimes an overlap in the regions some agencies work across, making analysis of this data more complex. When making or receiving a data sharing request, it is important everyone is aware of any limitations from misalignment of data sets and be very clear of the context in which the data is being presented. Questions to ask include: • Is data being shared in an accessible format? • Is the scope of the data set clear? • Does the data set contain all the information that is required for the identified purpose, or will there be a need to cross reference with additional data sets?
Terminology and Common Language for Data Sharing Requests	When making or receiving a data sharing request seek to validate the content. Different agencies may use different terminology for similar data sets, and unless the data is stored within a database, clear definitions steps will need to be taken to ensure that the data being shared will serve the purpose for which it is intended. Questions to ask include: • Is the request clear on the data that is required? • Do the data types meet requirements and contain the data that is needed? • Could challenges with the source of data collection cause discrepancies in the data that need to be highlighted?
Data Accuracy and Validation	Inaccurate data can cause delays and mean data is not available when needed. Taking reasonable steps to validate data will improve the quality of service across the CJS. Data Accuracy is a required principle and obligation for personal data processing, as set out in Annex 1.
Data Limitations	There may be instances where a data sharing request is made for a data set that is accurate but incomplete. In these instances, it is preferable to share the available data but with clear caveats about how to interpret it. • Be clear on what is and is not included in the data set and why • Consider whether missing data may result in unbalanced statistics or performance information; how can this be captured in the output to ensure missing information is considered? • Are time frames causing the issue? If the data sharing can be held off for an agreed period, would the resulting data set be more complete? Those engaged in the production of this guidance highlighted the value in ‘good enough’ data in terms of timeliness or completeness.

Part 3: How to Share Data with Confidence

Building on the foundations of good data sharing set out in Part 2, this section of the guidance sets out the practical steps, questions and considerations when actively looking to make or handle data sharing requests.

7 Practical Steps for Data Sharing

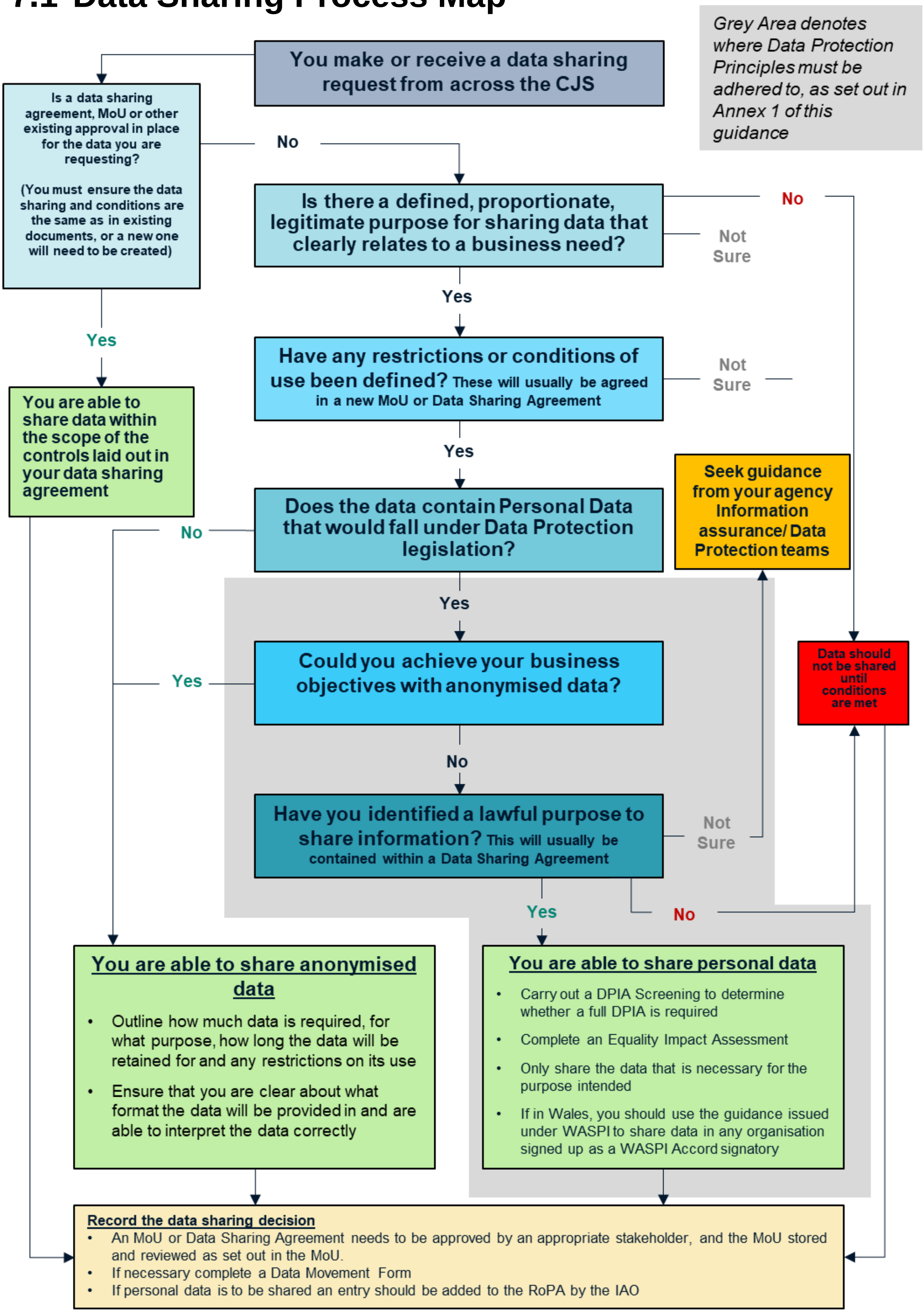
The following pages contain a step-by-step process flow for systematic, or regular sharing of data – with key questions to prompt the person requesting or sharing the data to ensure they understand how to share the data safely (and what to do if they cannot). This is supplemented by a checklist that provides further prompts to inform data sharing decisions. Section 8.3 below outlines ad-hoc data sharing requests.

The remainder of this section then provides further considerations with relation to:

- Data processing (in terms of frequency, volume, and timeliness);
- How to make a data sharing request;
- Resolving Data Sharing Disputes / Rejections.

In all these the purpose behind the data sharing request is key – a clear purpose is essential to justifying the request and scoping the data needed and how it is provided.

7.1 Data Sharing Process Map



Grey Area denotes where Data Protection Principles must be adhered to, as set out in Annex 1 of this guidance

You make or receive a data sharing request from across the CJS

Is a data sharing agreement, MoU or other existing approval in place for the data you are requesting?

(You must ensure the data sharing and conditions are the same as in existing documents, or a new one will need to be created)

Yes

You are able to share data within the scope of the controls laid out in your data sharing agreement

No

Is there a defined, proportionate, legitimate purpose for sharing data that clearly relates to a business need?

No

Not Sure

Yes

Have any restrictions or conditions of use been defined? These will usually be agreed in a new MoU or Data Sharing Agreement

Not Sure

Yes

Does the data contain Personal Data that would fall under Data Protection legislation?

No

Seek guidance from your agency Information assurance/ Data Protection teams

Yes

Could you achieve your business objectives with anonymised data?

Yes

Data should not be shared until conditions are met

No

Have you identified a lawful purpose to share information? This will usually be contained within a Data Sharing Agreement

Not Sure

Yes

No

You are able to share anonymised data

- Outline how much data is required, for what purpose, how long the data will be retained for and any restrictions on its use
- Ensure that you are clear about what format the data will be provided in and are able to interpret the data correctly

You are able to share personal data

- Carry out a DPIA Screening to determine whether a full DPIA is required
- Complete an Equality Impact Assessment
- Only share the data that is necessary for the purpose intended
- If in Wales, you should use the guidance issued under WASPI to share data in any organisation signed up as a WASPI Accord signatory

Record the data sharing decision

- An MoU or Data Sharing Agreement needs to be approved by an appropriate stakeholder, and the MoU stored and reviewed as set out in the MoU.
- If necessary complete a Data Movement Form
- If personal data is to be shared an entry should be added to the RoPA by the IAO

Fig 3: A process flow consolidating the information in this guidance that identifies the steps to take when data sharing. Once a data sharing request is received, it is necessary to determine whether it is a new request or will fall under existing agreements. It is important to determine whether the information contains personal data or not, and if it does, whether there is a lawful basis for this.

7.2 Data Sharing Checklist

The checklist below summarises the information provided in this guidance to ensure that all reasonable steps have been taken for the correct use and protection of data when data sharing. If there is any remaining concern about sharing data, seek advice from your agency Information Assurance / Data Protections leads.

Check whether you have identified a valid purpose for the data sharing	
What is the data sharing meant to achieve?	
Have you considered any potential risks to data sharing, and does the value or benefit gained from sharing outweigh risk? • *For personal data the principal focus here should be on risks to individuals whose data is shared; only if there is no personal data involved should corporate risks be prioritised.* • *Data sharing activities should undergo screening to determine whether a DPIA is required.*	
Is the sharing necessary and proportionate to the purpose you have identified for the data?	
Could the data be collected from an accessible dashboard?	
Could the objective of sharing be met by sharing a smaller data set, or by anonymisation of personal information?	
Have you identified processes which can be put in place to ensure data is shared safely? E.g. MoU, Data Sharing Agreement, limited system access.	
When you have decided to share	
What data will be shared?	
How will the information be shared?	
What agencies will be involved?	
What additional parties outside the MoU can the data be shared with – are there any third parties that have a business requirement to receive the data?	
What partnership boards can receive the data?	
Can the data be shared between PCCs across a single region?	
Have you identified an appropriate timeframe to share data?	
Have you ensured that you’ve identified and agreed appropriate technical resource to prepare the data that is being shared?	
What checks will be put in place to ensure the data being shared is sufficiently accurate for its purpose?	
Have security controls been identified?	

How will analysis be undertaken and findings be shared or validated?	
What is the agreed data retention period (if applicable)?	
When should regularly scheduled reviews of the data sharing take place?	
In addition to the above, for sharing Personal Data the Data Protection Principles must be adhered to (as described in Annex 1) - *Lawfulness, fairness and transparency* - *Purpose Limitation* - *Data Minimisation* - *Accuracy* - *Storage Limitation* - *Integrity and Confidentiality* - *Accountability*	
Have you determined any potential risk to the individual from sharing the data through a DPIA screening process?	
If so, have you consulted with your Data Privacy team to determine whether a DPIA is required?	
Have arrangements been clarified in an MoU or a Data Sharing Agreement?	
Has an Equality Impact Assessment been carried out? Have considerations been made relating to Special Category personal data (e.g., personal health data)?	
In Wales, have you used the WASPI resources to determine your approach to personal data sharing?	

The following sections provide more detail on the considerations needed to complete the steps in the process map and checklist.

7.3 Data Processing

When undertaking data sharing, processing considerations relating to frequency, volume and timeliness need to be addressed. You must set out and agree who is the Data Controller and who is the Data Processor when two or more organisations share data.

You're a <u>data controller</u> *if you're the main decision-maker when it comes to how people's personal information is handled, and how it's kept safe. Controllers can be a limited company, an organisation, charity, association, club, volunteer group or business of any size – including sole traders and people who work for themselves.*

You're a <u>processor</u> *if you're only acting on behalf of the instructions of a controller – if a business has hired you to process their mail, for example. As a processor, you wouldn't be doing anything with the data if the controller hadn't asked you to. It's not up to you to decide what should happen to it, which means you're only processing the information and not* *controlling it. However, you do have responsibilities to protect the personal data that you've been trusted with and to use it appropriately in-line with your contract with the controller.*

The difference between controller and processor is important because someone ultimately needs to be responsible for making sure personal data is handled lawfully, fairly, and transparently, that people are protected from harm and that their information rights are upheld.

Frequency of Data Sharing

Data sharing will either be ad hoc or part of a regular or systematic data sharing process:

- When making an ad hoc data request:
    - Be clear on the purpose that the data will be used for. Data may not be used for any purpose for which it was not agreed;
    - Consider how the data will be used in relation to the purpose and if it will be subject to further analysis;
    - If the data contains personal data:
        - Ensure the risks versus the benefit of sharing have been considered through DPIA screening/ a full DPIA, and there is a lawful basis for processing. Where personal data is shared as part of an ad-hoc request particular care should be given to ensuring legislation is adhered to, and if necessary, the Data Privacy team is involved in this process;
        - Anonymise data where possible (whilst still meeting its purpose). Consider whether the data is Special Category data.
    - Consider whether an MoU or Data Sharing Agreement may be required.

Volume of Data Sets

If a data set contains a large amount of information, it is important to ensure that only the information that is required for a specific business purpose is shared, especially in the case of personal data, where data minimisation is a fundamental principle. The more information that is handled, the greater the information management responsibilities. Key considerations here are:

- Clarity on the data required and the time for which the data will be needed;
- The scope of the data set needed to meet the purpose of the request i.e. is all the data needed or would a sub-set suffice;
- Whether the data required is accessible through an existing dashboard.

<u>NOTE:</u> Smaller anonymised data sets can run a risk of rendering data identifiable (and therefore personal and subject to UK GDPR/ DPA 2018).

<u>NOTE:</u> The principle of Data Minimisation as set out under GDPR is not only applicable to large data sets, but for any data collection/ sharing.

Timeliness and Relevance of Data

There is often a trade-off between the speed at which data can be shared and its relevance / accuracy and completeness. This impacts the quality of the data being received and could lead to misinterpretation of the data.

When requesting data consideration should be given to:

- The purpose of the data being requested and whether more timely / less accurate data is more beneficial:
    - Swifter data may be more helpful in identifying leading indicators and emerging issues;
    - Data that has been validated, verified, and published over a longer period is likely to be more useful for in-depth analytical purposes understanding what happened over time.
- Whether the necessary skills and measures are in place to handle the data safely.

In situations where agencies are sharing up to date but unpublished data, it is important that there is agreement on how the data will be analysed and used. Publication rights should remain with the organisation providing the data, unless agreed otherwise.

Where data is intended to provide performance management information, timeliness is considered more important than complete accuracy. Performance data based on returns from areas/establishments is therefore not subject to full checks which would delay its inclusion. For this reason, the accuracy of data cannot be guaranteed. Such data should not be used explicitly or implicitly in circumstances in which complete accuracy and certainty are required.

<u>NOTE:</u> Where personal data may be relevant, accuracy is an essential principle.

<u>NOTE:</u> Unpublished management information should not be released into the public domain prior to its use in the scheduled publication of official statistics unless explicitly agreed.

7.4 Making or Receiving Data Sharing Requests

Making a high-quality request for data is essential for enabling the recipient to approve and fulfil the request. Stakeholders engaged in the development of this guidance emphasised the need for a strong purpose and that the absence of this often led to delays or requests being rejected. What follows is a set of considerations to ensure a high-quality request is made.

When making or receiving a data sharing request, consider the following questions:

- How quickly is the data required?
- What is the impact if there is a time lag between the data being created and shared?
- Is the risk of a delay in receiving the data higher than the risk of the data being received in an unverified format?
- Is there an ideal timeframe from data creation to sharing of data that can be agreed between parties, that strikes a balance between timeliness, accuracy, and relevance?
- What time is needed for the request to be processed, documents signed off and agreed and access levels set up (if directly accessing a system or application)? The sharing organisation should be able to propose a timeframe for this process.

These questions assess the risk versus the benefit of data sharing within short timeframes:

- Where the benefit to receiving the data in a quicker turnaround outweighs the potential risk of data inaccuracy/ completeness, then the data may be shared but with a caveat that it has not been fully validated.
- Where the risk or impact of sharing data outweighs the benefits gained from it, alternate solutions should be sought, potentially including:
  - Agreeing to share the data within a longer agreed period;
  - Omitting a data set that may be inaccurate until these details have been verified (within an agreed timeframe);
  - Providing a high-level subset of the data initially and sharing the detail once it has undergone verification.

Identify the Data Being Requested

The data sets required need to be aligned to the business need (purpose) of the request – consider the following:

- What is the defined need for the data – how can the business benefit be quantified?
- Is the information accessible through an existing dashboard and is self-service an option?
- If the data is not yet fully validated (most likely for very timely data) consider whether:
  - The necessary analytical skills are in place to correctly interpret the data;
  - An incorrect conclusion / decision could be made from unprocessed or incomplete data that would then require further resource to rectify;
  - There is clarity on the caveats and requirements for working with unprocessed data, including limits on its use, handling and storage.
- Does the request cover data that contains personal data? If so, is this necessary for the purpose (or would anonymised suffice). If personal data is required UK GDPR/ DPA regulatory requirements apply, and screening should be undertaken to determine whether a DPIA is required and whether there are additional considerations for special category data (so time will need to be factored in for this).

- How to minimise the data being requested - which data elements are required to meet the business need, and can this be clearly communicated within an MoU or DSA?

When making a data request to other agencies, consider whether an additional MoU or other DSA is needed (if this is the first time that this data has been requested). Several MoUs already exist for data sharing, check to ensure this request is being made under the correct agreement.

Sharing Data

Where data sets do not include personal data, data sharing can often be carried out through agreed processes with minimal risk. An MoU will set out requirements for each party in relation to the handling of the data. New or one off / unusual requests should be reviewed by a suitable stakeholder.

Risks will increase where there is personal data involved, and a DPIA screening will be required if the data type has not previously been shared with the requestor or if there is a change to the processing needs set out in an existing DPIA.

When receiving a data sharing request, consider the following:

- Has a clear and justified business need been defined?
- Is the request proportionate to the business need?
- Is it clear exactly what is required from a data set – could a subset of data / anonymised data meet the request?
- Does the request require personal data? If so, adhere to the UK GDPR/ DPA regulatory requirements as set out **Annex 1**.
- How accurate will the data be when it is shared? Are specific handling arrangements required (e.g. that data is not shared in public if it has not undergone full analysis and or has not been published to an existing data dashboard).
- How easy is it to interpret the data? If a specific data set in raw format is unlikely to be of use for statistical purposes, it may be beneficial for the data to be analysed and checked prior to sharing.

Accessing Systems and Services for Data Sharing

Where a request is made for users to have access to systems or services to share data, there will be operational security considerations relating to what data needs to be accessed, under what conditions and by whom:

- Identify the user that requires access to the system;
- Determine what specific data sets or resources they require access to;
- Outline whether access should be read-only, or whether the user can edit or download data sets;

- Specify how long the user will require access to the data.

In most situations, we would not advise direct access to systems unless other mechanisms for data sharing will not be possible.

Where there is no alternative to systems access, consideration must be given to technical and procedural considerations. These will depend on the sensitivity of the data being shared and the level of attendant protections required, and might include things like:

- Two factor authentication;
- Role based access control;
- User training.

When Should Data Not Be Shared?

Data sets should not be shared between agencies before a MoU or DSA is in place, as this could leave parties at risk of mishandling the data. Additionally, where personal data is involved, data sets should not be shared until DPIA screening is completed. Before sharing, check whether a suitable agreement is in place. If it is not, build time into the process for this to be completed (the template MoU that accompanies this guidance should speed up the creation of new agreements).

An MoU or DSA will determine the boundaries of what data can be shared, and how that data can be used. There may be restrictions within the MoU or DSA on further sharing of data to other parties or public, and these should be adhered to.

7.5 Resolving Data Sharing Disputes / Rejections

Each agency should already have a documented resolution process as part of Information Assurance / Data Protection governance, and these should be followed. For data sharing where an MoU or DSA is implemented these documents will clearly outline a resolution process to be followed based on the agency process. The MoU will include roles, responsibilities and contact details.

In most cases, data sharing disputes or rejections can be resolved through transparency of data use and the implementation of handling conditions.

If there is a dispute, consider the following:

- Revisit the **justification** for data sharing, ensure it remains valid and the scope of the request is clear. Consider whether a subset of the data set might suffice (is there a particular part of the data set that is causing the obstruction);
- Where the request is under an MoU or DSA, ensure that the document has been **correctly completed** and includes clear escalation routes for disputes;
- Be clear on any **restrictions on the use of the data** and ensure both parties are aware of these.

ANNEXES

Annex 1: Data Privacy Regulations

The UK GDPR and DPA 2018 set out conditions for the processing of personal data. The purpose of these regulations is to ensure that personal information is handled in a controlled, secure manner to protect the information of individuals, or data subjects. **The regulations must be followed when handling personal data.**

Failure to handle personal information correctly could lead to an information breach, loss of access to vital personal information, or information being incorrectly amended. All of these could impact on the safety or wellbeing of the individual. In the UK, the Information Commissioners Office (ICO) regulates data protection, offering advice and guidance, promoting good practice, monitoring compliance, and taking enforcement action, where appropriate.

The UK GDPR sets out six data protection principles to be considered when handling **personal data:**

1. **Lawful, fair, and transparent processing:** clear, open and honest about what personal data is processed and what it is processed for. Only handling personal data in the ways that people would expect. This means that identifying a lawful purpose for the processing of personal data.
2. **Purpose limitation:** the processing of personal data must be for a specified, explicit and legitimate purpose. If personal data is to be used for a different purpose from the one it was collected for, the new purpose must be compatible with the original purpose
3. **Adequate, relevant, and not excessive:** often referred to as 'data limitation', this is about ensuring that the data processed is of sufficient relevance and is not more than needed.
4. **Accuracy:** ensure the source and status of personal data is clear in the records to ensure its accuracy, Including being kept up to date where necessary (DPA 2018 s. 38(1)(a))
5. **Storage Limitation** - personal data should not be kept for longer than is necessary for the purpose for which the personal data is processed.
6. **Security** - have appropriate security in place to take account of the risks of processing personal data. For example, to prevent the personal data processed from being accidentally or deliberately compromised.

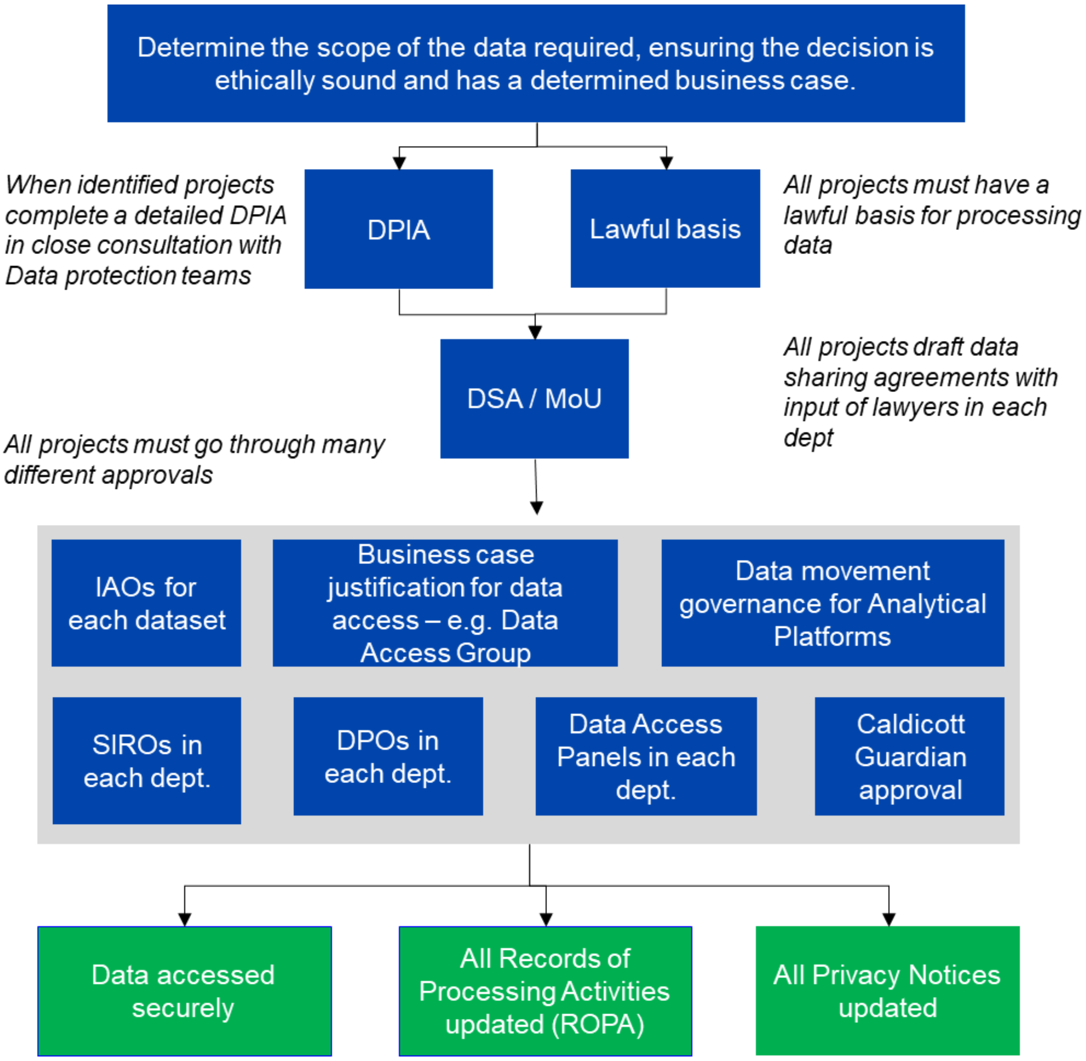
You may hear reference to Data Processors and Data Controllers. The ICO has produced guidance about these roles, which can be found here Controllers and processors | ICO

The table below sets out specific considerations relating to the handling of personal data in the CJS:

Specific consideration	Guidance
Law Enforcement Processing of Personal Data	Not all personal data can be obtained or used with the consent of the individual. This is particularly the case where data is collected and shared for the purposes of law enforcement. **The DPA Part 3 sets out how to correctly process data for law enforcement purposes**. Agencies and authorities that process data for law enforcement purposes are known as 'competent authorities' under the DPA. Competent authorities may process for purposes other than law enforcement, but are nevertheless competent authorities. Bodies which are not competent authorities cannot process for a law enforcement purpose (except where the data subject has given consent for the processing). The purpose for processing defines the regime under which the data is processed, but not the status of the body doing the processing.
Data Sharing Agreements	If the data required contains personal information a **Data Sharing Agreement (DSA) is required**. A DSA should list any controls or considerations relating to the management of personal data. Once in place, further approval for data sharing is not necessary unless the data or how it is processed varies from the scope of the original agreement. **Ad-hoc requests** for personal data can be carried out without a DSA, provided there is a clear understanding of the business need for the data and awareness of the handling and use of the data. Responsibilities around personal data: • **When making a request** for data sets that contain personal data, a clear case must be provided, ensuring the data protection principles have been addressed. • **When receiving a request** for personal data the recipient must ensure that the data protection principles have been considered. • Undertake DPIA screening to determine whether a full Data Protection Impact Assessment (DPIA) is required – see below.
Data Protection Impact Assessments (DPIA)	If there is a need to share personal data regularly with another body and agreements are not already in place with or are wanting to share a different type of data set, **Data Protection Impact Assessment (DPIA)** may be needed. DPIA screening should always be carried out to determine whether a full DPIA is required. The purpose of the DPIA is to describe the data processing, describe the risks to the individual and record mitigations in place to adequately lower the risk. Failure to complete a DPIA where one is required is a breach of ICO requirements. The local Data Protection Office can provide support around when a DPIA may be required, and the process to complete one.

	If the particular example of data sharing does not put the individual or individuals' data that is being shared at high risk, then a DPIA may not be required.
Support with UK GDPR and DPA 2018	The ICO need to be involved where the DPIA indicates that the processing would result in a high risk to the rights and freedoms of individuals. Local data protection teams should consult with the ICO where necessary during this process and the ICO will work with those teams to find a workable solution.
Support with Data Privacy	Agencies will have an information assurance/ information security or data privacy team dedicated to ensuring UK GDPR and DPA regulations are met. Check locally whether there is a DPO or Key point of contact for information management (e.g. Data Custodian) that can help with data sharing questions in relation to personal data. As above, a Data Protection Officer (DPO) may need to be involved if personal data is to be shared personal data. For general information relating to data sharing and for more detail on the data protection principles, visit the Information Commissioners Office (ICO) website, which gives guidance for organisations processing personal data.

The diagram below shows a typical governance process for sharing personal data, showing the different steps and documentation that may be required. The diagram is illustrative only, and you should always consult with your data privacy team or DPO when sharing personal data to ensure you are compliant with data protection legislation.



Determine the scope of the data required, ensuring the decision is ethically sound and has a determined business case.
When identified projects complete a detailed DPIA in close consultation with Data protection teams
DPIA
Lawful basis
All projects must have a lawful basis for processing data
DSA / MoU
All projects draft data sharing agreements with input of lawyers in each dept
All projects must go through many different approvals
IAOs for each dataset
Business case justification for data access – e.g. Data Access Group
Data movement governance for Analytical Platforms
SIROs in each dept.
DPOs in each dept.
Data Access Panels in each dept.
Caldicott Guardian approval
Data accessed securely
All Records of Processing Activities updated (ROPA)
All Privacy Notices updated

Fig 4: A diagram showing a typical governance process for data sharing.

In the case of Welsh personal data, the diagram in the following link can be used can be used to establish the approach to take under WASPI: What agreement is required? - Welsh Accord on Sharing of Personal Information (gov.wales) .

Annex 2: Glossary of Terms

Anonymise	A process which blocks or eliminates personal information and cannot be reversed back into personal data at any point or combined with other data sets to identify an individual.
Criminal offence data	Personal data relating to criminal convictions and offences or related security measures. For example, it can also cover suspicion or allegations of criminal activity. You are more likely to need to do a DPIA for processing criminal offence data as it is likely to be high risk.
Data Controller	A data controller has the responsibility of deciding how personal data is processed and protecting it from harm.
Data Processor	Data processors have to protect people's personal data – but they only process it in the first place on behalf of the controller. They wouldn't have any reason to have the data if the controller hadn't asked them to do something with it.
Data Protection Act 2018 (DPA 2018)	Governs the processing of information relating to living individuals, which is known as 'personal data'. It provides individuals with a number of important rights to ensure that personal data covered by the DPA is processed lawfully. In general terms the DPA regulates the manner in which personal data can be collected, used and stored. Part 3 regulates the processing of personal data for 'Law Enforcement Purposes' and is the part which applies to Operational Information. See also UK GDPR.
Data set	A data set is a collection of information in electronic form to do with the services and functions of an agency that is neither the product of analysis or interpretation, nor an official statistic and has not been materially altered.
Data Subject	An identified or identifiable living individual to whom personal data relates.
Deletion	The permanent disposal of a record by its removal from electronic systems to the extent that it cannot be re-accessed other than by the application of specialist techniques not available in the ordinary conduct of business.
Destruction	The permanent disposal of records that are no longer required for a business purpose, beyond any possible reconstruction. This term refers to hard copy records where these are erased irretrievably.
Disposal	The stage in the lifecycle of a record where the record is judged whether it should be retained (for business or historical purposes) or destroyed in line with an agency's Retention Schedule.

General Data Protection Regulation (UK GDPR)	Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data. This EU legislation expands the rights of individuals to control how their personal information is collected and processed, placing a range of new obligations on organisations to be more accountable for data protection. See also DPA 2018.
Information Asset Owners (IAO)	A named individual with responsibility for the information created, obtained and retained in their business areas, office locations and designated applications and systems. They are responsible for leading on Information Governance, improvements, and understanding of the assets in their remit. They assure the accuracy of the Information Asset Register (IAR), its alignment to their business functions and its compliance within any legal criteria. IAO's are also accountable for data sharing processes and documents such as MoU's, DSA's and DPIA's.
Information Asset Register (IAR)	An IAR is a simple way to enable the Agencies to understand and manage information assets and the risks to them. IARs are common across HMG and the UK public sector as a key component of Information Management and Governance. It is a key tool for fully exploiting information assets and, when completed and updated accurately, it helps identify areas of duplication, identifies senior risk ownership of information and encourages greater efficiency. It can be used to spot areas of potential risk and the need for improvement. By understanding the nature of Agencies information and where it's hosted, effective risk management is more easily enabled. The IAR is owned by the Agencies Senior Information Risk Officer (SIRO). The IAR is reviewed by IAOs, Information Custodians and the Data and Information Lifecycle Management team in the Chief Data Office (CDO) in support of the SIRO performing their role and responsibilities.
Information Commissioner's Office (ICO)	UK authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals.
Information Custodian (IC)	A role that may be appointed by an IAO to act as a Single Point of Contact (SPoC) in a business delivery area for information governance and management within a specific business area.
Law Enforcement Purposes	The Law Enforcement Purposes are defined in Part 3, Chapter 1, s31 of DPA 2018 which states: "The law enforcement purposes: For the purposes of this Part, "the law enforcement purposes" are the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security." When a competent authority processes personal data for a law enforcement purpose, Part 3 DPA 2018 applies; a competent authority processing for a purpose other than law enforcement will process under UK GDPR, likewise a body which is not a competent authority cannot process under Part 3 but

	will process under UK GDPR (where the data subject has given consent for the processing).
Operational Information	Information processed for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties. Operational Information that also contains Personal Data (which it very commonly will) is the same as the information which is governed by Part 3, 'Law Enforcement Processing' of DPA 2018.
Personal Data	Any information relating to an identified or identifiable living individual'. "Identifiable living individual" means a living individual who can be identified, directly or indirectly, in particular by reference to— (a) an identifier such as a name, an identification number, location data an online identifier, or (b) one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the individual. (DPA 2018)
Personal Data Breach	'A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed' (Article 4, UK GDPR). Personal Data Breaches are a form of security incident/information breach.
Personal Data Processing	An operation or set of operations which is performed on personal data.
Processing likely to result in high risk	Examples of such processing include but are not limited to- Use of innovative technology, large-scale profiling, biometric data, genetic data, data matching, invisible processing, tracking, targeting of children or other vulnerable individuals, risk of physical harm to data subjects.
Pseudonymisation	'The processing of personal data 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 subject to technical and organisational measures to ensure that personal data is not attributed to an identified or identifiable individual' (DPA 2018). To be clear, this is different to anonymisation (where the data is scrubbed for any information that may serve as an identifier of a data subject). Pseudonymisation is a type of processing designed to reduce data protection risk but not eliminate it; it should be thought of as a security and risk mitigation measure, not as an anonymisation technique by itself. Pseudonymised data is still subject to data protection legislation.
Records of Processing Activity (RoPA)	The record of processing activity allows an organisation to make an inventory of the data processing functions and activities and to have an overview of what the organisation is doing with the personal data it holds

	and who it is sharing it with. The recording obligation is stated by Article 30 of the UK GDPR and is supplemented by the DPA 2018.
Retention Period	The length of time after a document is closed that it needs to be retained before being reviewed (this can include records and non-records).
Retention Schedule	A document which sets out the periods by when different classes of information must be formally reviewed to determine if they can be further retained or disposed of. A records retention schedule is obligated under Article 30 of UK GDPR.
Sanitisation of Information	The removal of references from the content of records containing intelligence material which explicitly or implicitly reveal the nature or identity of its source, e.g. technical or Covert Human Intelligence Sources or particularly sensitive information which requires careful handling.
Special Category Data (excluding data under Pt3)	The UK GDPR defines special category data as: - Personal data revealing racial or ethnic origin - Personal data revealing political opinions - Personal data revealing religious or philosophical beliefs - Personal data revealing trade union membership - Genetic data - Biometric data - Data concerning health - Data concerning a person’s sex life - Data concerning a person’s sexual orientation This does NOT include personal data about criminal allegations, proceedings or convictions (Criminal offence data), as separate rules apply.
Third Party	1: A person who is not an agency employee. 2: ‘Third party’ is defined in DPA 2018 for the purposes of para. 6 of Sch. 9 (the legitimate interests data processing condition).
Version Control	The management of changes to documents.

Annex 3: Sources of CJS Data

The ‘CJS Delivery Data Dashboard’ brings together data from partners across the CJS presenting data in an accessible format from the police, CPS and the courts. It is published quarterly: https://criminal-justice-delivery-data-dashboards.justi The ‘CJS Delivery Data Dashboard’ brings together data from partners across the CJS presenting data in an accessible format from the police, CPS and the courts. It is published quarterly: https://criminal-justice-delivery-data-dashboards.justice.gov.ukce.gov.uk

The ‘Crown Court Information Tool’ displays data on all Crown Courts in England and Wales and provides an overview for key statistics for workload, disposals by offence group, average duration and number of hearings by disposal group, waiting times, trial outcome reasons and outstanding cases. It is updated quarterly.

https://public.tableau.com/app/profile/moj.analysis/viz/CrownCourtinformationJune2022/Introduction

The ‘Criminal Court Statistics’ presents the latest statistics on type and volume of cases that are received and processed through the criminal court system of England and Wales. The figures give a summary overview of the volume of cases with statistics broken down for the main types of cases involved. Also published are detailed breakdowns of the headline court caseload and timeliness statistics, broken down by court or Local Justice Area. It is updated quarterly.

https://www.gov.uk/government/collections/criminal-court-statistics

The ‘Criminal Justice Statistics Quarterly displays trends in the use of out of court disposals, defendants prosecuted, offenders convicted, remand and sentencing decisions and offender histories at a national level across England and Wales. Pivot tools are published that allow users to break down the statistics by Police Force Area and other characteristics such as offence, age, and ethnicity. It is published quarterly.

https://www.gov.uk/government/collections/criminal-justice-statistics-quarterly

The ‘Women and the Criminal Justice System’ publication compiles statistics from data sources across the CJS, to provide a combined perspective on the typical experiences of females who come into contact with it. It considers how these experiences have changed over time and how they contrast to the typical experiences of males. It is updated bi-annually, alternating with the ‘Ethnicity and the Criminal Justice’ System publication.

https://www.gov.uk/government/statistics/women-and-the-criminal-justice-system-2021

The ‘Ethnicity and the Criminal Justice System’ publication compiles statistics from data sources across the CJS, to provide a combined perspective on the typical experiences of different ethnic groups. It considers the over- representation of minority ethnic groups at many stages throughout the CJS when compared with the White ethnic group. It is updated bi-annual, alternating with the ‘Women and the Criminal Justice System’ Publication.

https://www.gov.uk/government/statistics/ethnicity-and-the-criminal-justice-system-statistics-2020/ethnicity-and-the-criminal-justice-system-2020

The Youth Justice Board publishes the 'Youth Justice Annual Statistics' and experimental statistics such as 'Assessing the Needs of Sentenced Children in the Youth Justice System'. This includes data on the use of remands, children in youth custody and behaviour management in the Children and Young People Secure Estate. These statistics are published annually and include local level pivot tables.

Youth justice statistics - GOV.UK (www.gov.uk)

The 'Safety in the Children and Young People Secure Estate Report' contains data on assaults, self-harm and deaths in the Children and Young People Secure Estate. In 2023, it will be expanded to include data on Separations and Use of Force. It is published quarterly.

Safety in the Children and Young People Secure Estate: Update to June 2022 - GOV.UK (www.gov.uk)

The 'Youth Custody Data Report' is a snapshot of all children and young people in the Children and Young People Secure Estate on the last day of the month. It contains breakdowns by sector type, ethnicity, gender, age, region of Youth Justice Services, region of Establishment, offence group and distance from home bands. It is published monthly.

Youth custody data - GOV.UK (www.gov.uk)

The 'HMCTS Weekly External MI – Crime dashboard' is a bespoke dashboard covering Crown and Magistrates' jurisdictions and includes a variety of workload metrics. It is updated each Monday. Requests for access should be made via:

Analysis & Performance - Data Request form (office.com)

The 'HMCTS Trials - External MI dashboard' provides case-level trial outcome reasons for Crown and Magistrates' Courts. It is updated on a monthly basis. Requests for access should be made via:

Analysis & Performance - Data Request form (office.com)

HMCTS provide two dashboards of local MI that are not subject to the same quality assurance as official statistics. Data from these dashboards must therefore not be shared or published externally. This page summarises the statistics available:

Statistics at MOJ - Ministry of Justice - GOV.UK (www.gov.uk)

In Wales, the Secure Anonymised Information Linkage (SAIL) Databank brings together a repository of anonymised data, including data on Health, the Criminal Justice System, Education, Social Care and data from the Census. SAIL is the Welsh Government's preferred mechanism for securely providing data to researchers for linked data analysis. Requests to work with the data can be made via:

Apply to work with the data - SAIL Databank