

Breaking down barriers: Implementing effective multi-agency data sharing

White paper

*He's barely in
class. There's a
history of*

EDUCATION
Data source

**drugs offences
in the family.**

YOUTH CRIME
Data source

**Signs of
bruising and**

SOCIAL CARE
Data source

**risk of being groomed
to sell drugs.**

YOUTH CRIME
Data source



Executive summary



David Tonks

Lead for Policing & Justice, Capita



Stan Gilmour KPM

Business Consultant, Policing & Justice

The case for change: Why data sharing still fails

Despite robust legislation and decades of policy commitment, UK public sector organisations continue to face systemic barriers to effective information sharing across agencies. From the case of Victoria Climbié to the Radubukana case, serious safeguarding failures have repeatedly exposed how siloed systems, inconsistent risk assessments, and professional hesitancy can allow preventable harm to occur. The need for a secure, proactive and joined-up data sharing model has never been more urgent.

This white paper is presented in two halves. The first half sets out the need for multi-agency data sharing (MADS), drawing on evidence from serious case reviews, statutory duties, and frontline challenges. It highlights the limitations of current practice, including ad-hoc data exchanges, outdated technical infrastructure, and risk-averse interpretations of data protection law.

These issues are compounded by professional silos, incompatible IT systems, and fragmented governance structures that often leave agencies reacting to crises rather than preventing them.

What good looks like: Secure, scalable and ethical sharing

The second half of the paper explores the emerging capabilities that make secure, scalable, and preventative data sharing not only possible, but increasingly essential. Security and accessibility are at the core of a modern MADS capability, which includes:

- **Secure cloud-based infrastructure** with near real-time data sharing, access by authorised users, role-based access controls, and end-to-end encryption.
- **Common Data Model (CDM)** enables unified structures that support data consistency, simplified management, and enhanced analytics.
- **Standardised data formats and risk frameworks**, enabling cross-sector consistency and more reliable decision-making.
- **Comprehensive audit trails**, privacy-by-design features, and automated compliance checks to build confidence in ethical and lawful data use.

But technology alone is not enough. This white paper presents a holistic framework for successful implementation, recognising that culture, governance, and leadership are just as vital as infrastructure. It advocates for:

- **Clear information governance protocols** that balance the duty to protect with the obligation to share.
- **Ethical decision-making frameworks** to guide professionals in real-world safeguarding scenarios.
- **Cross-agency leadership and culture change** programmes to overcome mistrust, misinterpretation, and inertia.
- **Sustainable partnership models** with shared accountability, joint investment, and regular review cycles.

From vision to delivery: A proven and supported path forward

The implementation roadmap follows a phased approach, starting with foundational governance, progressing through deployment of priority sharing capabilities, extending to wider agency participation, and maturing into advanced analytics for predictive intervention. This can be delivered either through a self-managed programme or via a fully supported managed service, significantly reducing technical and organisational complexities while accelerating benefits.

The benefits of MADS are profound with earlier interventions, reduced duplication, more precise resource allocation, greater professional confidence, and a measurable shift from reactive to preventive practice. By integrating people, processes, and technology into a cohesive operating model, MADS provides a clear pathway to safer communities, more resilient services, and improved outcomes for the most vulnerable.

The MADS capability: Designed for impact

In partnership with police forces and local authorities, we have developed a transformative multi-agency data sharing (MADS) capability and supporting operating model. This addresses key technical and cultural barriers while supporting specialist functions such as data governance, data mastering, data pipeline management, analytics and data visualisation.

Built on a cloud-first architecture and delivered as a fully managed service, our MADS capability removes the technical burden typically associated with large-scale IT deployments. It accelerates implementation timelines, reduces cost, and ensures sustained value through continuous improvement and expert guidance from our Centre of Excellence for Data Sharing.

If your organisation is exploring how to improve data sharing across agencies or partnerships, we welcome the opportunity to share insights, case studies, and approaches that have worked successfully. For more information or to start the conversation with our team, visit content.capita.com/MADS or e-mail bettergovernment@capita.com.

1

Introduction



1

Introduction

The effective sharing of information between criminal justice services and community safety partners has long been recognised as essential to preventing harm and protecting vulnerable individuals. Yet, despite this recognition, the UK continues to experience a troubling pattern of information-sharing failures that have contributed to avoidable tragedies.

From the death of Victoria Climbié in 2000 to the more recent case of Arthur Labinjo-Hughes in 2021, serious case reviews have consistently identified breakdowns in multi-agency communication and failure of information sharing as a critical factor.



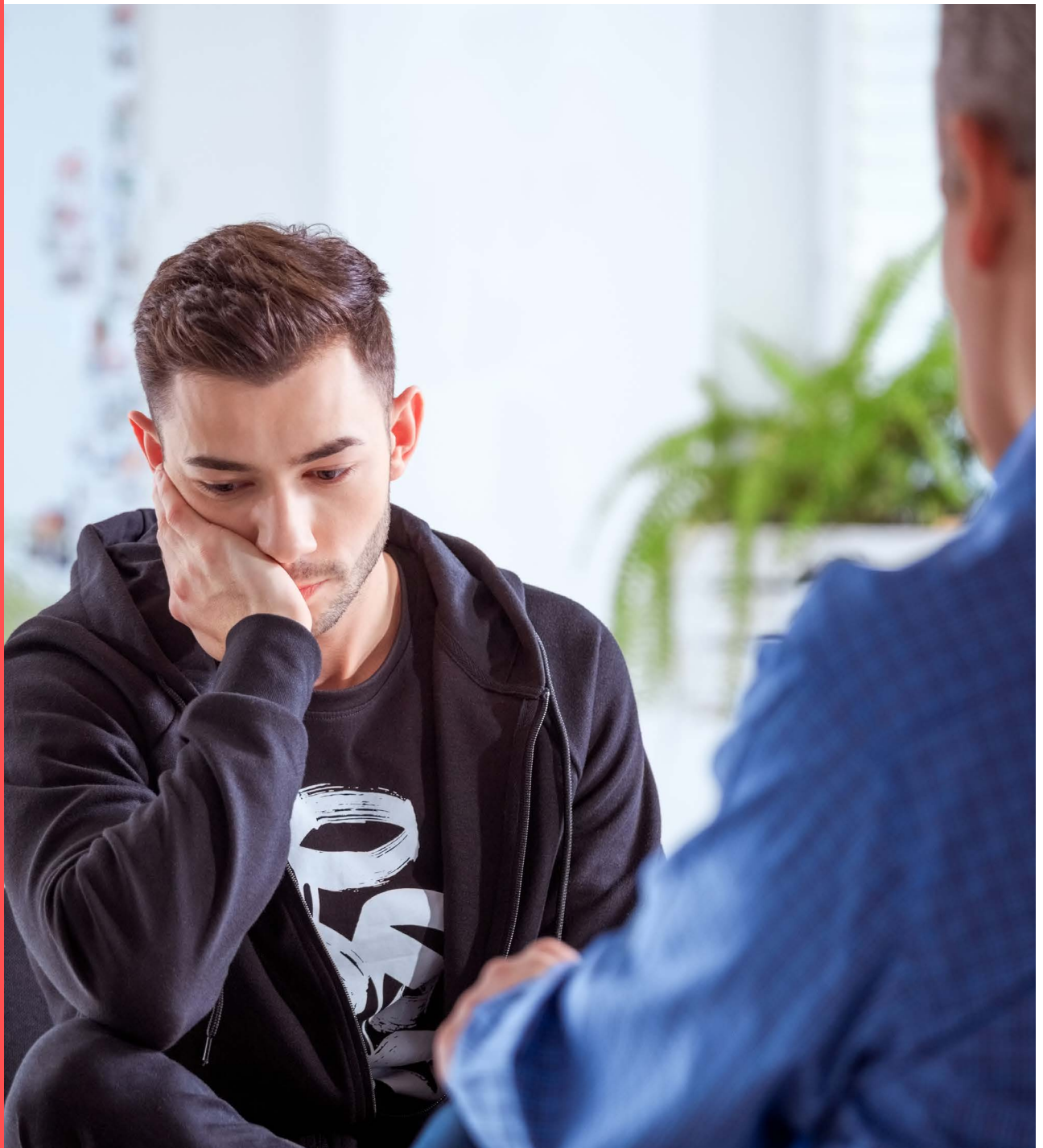
These failures are not isolated incidents, but symptoms of deeper, systemic issues. Siloed data systems, inconsistent risk assessment frameworks, and professional uncertainty about legal thresholds for information-sharing, all contribute to missed opportunities for timely intervention. This white paper aims to:

- Examine the historical context and legislative framework for information sharing in safeguarding.
- Analyse the persistent challenges that continue to impede effective multi-agency collaboration.
- Explore how technological solutions, particularly in the form of a MADS capability, can help address these barriers.
- Outline the operational and economic benefits of effective multi-agency data sharing.
- Provide a practical framework for implementation, grounded in real-world needs and constraints.

As safeguarding professionals and organisations navigate increasingly complex operational environments, the case for effective information-sharing systems has never been stronger. However, to date proven solutions and supporting services have remained elusive. This paper offers a clear path forward, grounded in insight, evidence and emerging digital capabilities, to help agencies break down barriers and better protect vulnerable individuals.

2

Historical context and problem statement



2

Historical context and problem statement

2.1. Historical failures in information sharing

The UK's safeguarding landscape has been shaped by a series of tragic events that exposed critical weaknesses in multi-agency collaboration. Lord Laming's 2003 inquiry into the death of Victoria Climbié identified catastrophic communication failures across agencies. Similar findings emerged in the reviews of Peter Connelly (2007), Daniel Pelka (2013), and more recently Star Hobson (2020) and Arthur Labinjo-Hughes (2021).

The 2024 Radubukana case in Southport further highlighted that despite legislative and policy reforms, fundamental problems with proactive information sharing between public sector organisations and agencies continue – especially around risk recognition and contextual understanding.

Across these cases, common themes persist: missed opportunities for intervention prior to risks crystallising, gaps in multi-agency communication, siloed data systems, and uncertainty around sharing responsibilities.

2.2. Inadequate multi-agency data sharing

Data held across government agencies, including local authorities, police, education and health services, has predominantly been shared in a reactive manner. Rather than being guided by proactive, systematic protocols, agencies often exchange data only after a specific concern emerges.

This reactive approach frequently results in harm – vulnerable individuals fall through the cracks, and services become crisis-driven rather than preventative. The absence of pre-emptive data flows contributes to repeated cycles of victimisation and offending, straining systems designed to protect the public.

2.3. Consequences of ineffective data sharing

The consequences of data-sharing failures are wide-ranging and well-documented:

- **Increased risk of harm:** Many serious case reviews have found that incomplete information sharing contributes to avoidable tragedies. Both the Independent Review of Children's Social Care and the Child Safeguarding Practice Review Panel have emphasised its importance for achieving better outcomes for vulnerable children and families.
- **Missed opportunities for timely interventions:** Particularly in domestic abuse cases, delays in sharing risk-related data have led to preventable escalation and ongoing harm, as evidenced in Domestic Homicide Reviews.
- **Compromised decision-making processes:** Incomplete, outdated, or siloed data undermines the effectiveness of safeguarding and community safety strategies.
- **Predominance of reactive measures:** Without integrated data flows, early warnings are missed, and responses remain reactive rather than preventative.
- **Perpetuation of social inequalities:** Poor data visibility makes it harder to identify and address systemic disparities, especially among marginalised communities.
- **Fragmentation of support systems:** Individuals experiencing overlapping issues (e.g. mental health and substance misuse) are often failed by disjointed systems.
- **Failure to reduce reoffending:** Gaps in data sharing prevent meaningful rehabilitation or coordinated interventions for offenders, particularly in domestic violence cases.

2.4. Legislative framework: Powers are in place

The UK has an extensive legal foundation that permits and, in many cases, mandates multi-agency data sharing:

- **Children Act 1989 and 2004:** Duty to cooperate to improve children's wellbeing.
- **Care Act 2014:** Adult safeguarding responsibilities.
- **Digital Economy Act 2017:** Legal gateways for public sector data sharing.
- **Police Reform and Social Responsibility Act 2011:** Framework for Police and Crime Commissioners governance.
- **Police, Crime, Sentencing and Courts Act 2022:** Introduced the Serious Violence Duty, marking a significant step forward in information sharing by requiring specified authorities to share data, collaborate on prevention strategies, conduct local needs analysis, and held accountable for failures to act on serious violence.

These are supplemented by statutory guidance such as "Working Together to Safeguard Children 2023" and guidelines from the Information Commissioner's Office on data sharing.

2.5. Why are legal powers alone are not enough

Despite a robust legislative foundation, barriers to effective multi-agency data sharing persists due to:

Misinterpretation and excessive caution

- **Risk-averse interpretation:** Many agencies often interpret UK GDPR and the Data Protection Act 2018 too conservatively, fearing legal consequences of sharing more than those of not sharing.
- **Complexities and competing frameworks:** The interplay of safeguarding, privacy, and crime prevention legislation leads to confusion and hesitation.

Organisational and cultural barriers

- **Professional silos:** Different terminologies, standards, operating models and risk thresholds impede effective communication and collaboration.
- **Lack of trust between agencies:** Concerns about how information might be used, stored, or interpreted by other agencies create reluctance to share beyond organisational boundaries.
- **Power imbalances:** Differential status, resources, and influence among partner agencies can distort sharing relationships. More powerful agencies may dominate information flows, while smaller partners may feel their contributions are devalued or their information needs neglected.

Practical and technical constraints

- **Incompatible data systems:** Many public sector organisations operate legacy IT systems that cannot easily communicate with each other. The absence of standardised data formats, identifiers, and interfaces creates significant technical barriers to routine information exchange.
- **Resource constraints:** Effective data sharing requires investment in technology, training, and dedicated staff time. In a context of austerity and resource scarcity, these investments have often been deprioritised.
- **Lack of data quality standards:** Inconsistent approaches to data collection, validation, and management create concerns about the reliability and utility of shared information. This undermines confidence in the value of data sharing arrangements.

Governance and leadership deficits

- **Inadequate leadership commitment:** Senior leadership across agencies have often struggled to prioritise data sharing or create the necessary conditions for it to flourish. Without championing at senior levels, information sharing initiatives struggle to gain traction.
- **Fragmented governance:** The responsibility for enabling data sharing is frequently dispersed across multiple governance structures with unclear accountabilities. This creates coordination problems and allows systemic barriers to persist unaddressed.
- **Insufficient performance incentives:** Existing performance frameworks rarely measure or reward effective information sharing. Without clear incentives, the additional effort required for systematic sharing is easily displaced by more visible priorities.

2.6. Implications for the future

The persistent disconnect between legal provisions and operational reality highlights key lessons in policy and practice:

- **Implementation support is essential:** Legislation alone won't change practice without investment in tools, training, and coordination.
- **Cultural change requires sustained commitment:** Shifting from risk-averse to appropriate sharing cultures demands long-term commitment to training, leadership development, and cross-agency relationship building.
- **Technology is foundational:** Modern, secure, interoperable infrastructure is no longer optional, it's critical and practical.
- **Accountability must evolve:** Regulators and inspectorates should include information-sharing effectiveness in their assessments.

2.7. Problematic practices to avoid

Current operational data sharing methods frequently rely on outdated approaches that undermine both security and analytical potential. To modernise data sharing, it is essential to explicitly move away from the following flawed approaches.

Insecure transfer mechanisms

- **Spreadsheets via email:** Widely used but highly insecure, this method creates risks around version, data leaks and unauthorised access.
- **Emailing sensitive data:** Despite clear guidance against it, email remains a common channel for sharing sensitive information.
- **Physical media (USBs, external drives):** Transfers via removable storage introduces threats of data loss, theft, or introduction of malware into secure networks.
- **Weak encryption and access controls:** Where digital transfers are used, they are often inadequately protected – relying on shared passwords or unsecured links.

Methodological limitations

- **Black box extraction algorithms:** These automated processes select data based on narrowly defined parameters. These often exclude contextual information, professional judgements, and qualitative insights that don't fit the predefined criteria but may be crucial for comprehensive risk assessment.
- **Static point-in-time snapshots:** Current practices typically capture information at a specific moment rather than providing continuous visibility of changing circumstances. This static approach fails to reflect the dynamic nature of vulnerability and risk.
- **Loss of context:** When extracting data from case management systems, vital contextual information is often lost, reducing complex situations to simplified data points that may mislead recipients about the true nature of risks or needs.
- **Inconsistent definitions:** Key terms such as "risk level" vary widely between agencies, making comparisons misleading and dangerous.

Governance and control issues

- **Loss of data ownership and oversight:** When data is transferred between agencies via spreadsheets or similar mechanisms, the originating agency loses visibility of how their information is subsequently used, interpreted, or further shared.
- **No audit trail:** Traditional sharing methods provide limited or no capability to track who has accessed shared data, how it has been used, or whether it has been appropriately deleted when no longer required.
- **Duplicate data sets:** The practice of sharing via data extracts creates multiple copies across different systems, leading to version control problems and increasing the risk of outdated information informing critical decisions.
- **Limited of revocation controls:** Once data is shared via traditional methods, the originating agency typically has minimal ability to restrict access to specific authorised individuals or revoke access when no longer appropriate.

Analytical constraints

- **Barriers to real-time insight:** Manual data sharing introduces lag, undermining time-sensitive decision-making.
- **Poor integration potential:** Spreadsheet-based sharing fundamentally limits the ability to dynamically combine data from multiple agencies to identify complex patterns of risk or need that span organisational boundaries.
- **Restricted analytical capabilities:** Basic data transfer methods limit recipients to using generic tools for analysis rather than specialised analytical capabilities that could extract more valuable insights.
- **No visibility of evolving patterns:** Static data sharing impedes the identification of temporal patterns or escalating concerns that might only become visible through continuous monitoring of changing circumstances.

2.8. New approaches for modern data sharing

Future multi-agency data sharing would include:

- **Secure cloud-based platforms** where data remains under originator control while authorised partners can access insights without taking possession of raw data.
- **Leading data pipeline solutions and data management techniques** enabling greater confidence in the ability to manage data using industrial tools and proven specialist working practices.
- **Standardisation of approach** supporting improved collaboration, reuse and reduced waste associated with bespoke solutions.
- **Efficient, secure and standardised processes** for ingesting source data.
- **Federated analysis models** that enable cross-dataset analysis while data remains within its original secure environment.
- **Role-based access controls** that restrict visibility to the minimum necessary information based on specific professional needs.
- **Near real-time data visibility** ensuring decisions are based on current rather than historical information.
- **Comprehensive audit capabilities** tracking all access and use of shared information.
- **Standardised data models** with consistent definitions and classifications across partner agencies.

These approaches would maintain appropriate security and governance while enabling the analytical depth necessary for effective safeguarding and early intervention.

3

Advantages of multi-agency data collaboration



3

Advantages of multi-agency data collaboration

Effective multi-agency data sharing unlocks significant opportunities across public services. When information flows securely and seamlessly between partners, each agency is better equipped to fulfil its role in safeguarding, prevention and community safety.

3.1. Local authority opportunities

- **Forecasting and prevention:** Use historical crime, demographic and socioeconomic data to identify high-risk areas for targeted interventions.
- **Vulnerability assessments:** Combine data sets to pinpoint individual and communities at risk of exploitation, neglect or social exclusion.
- **Housing and social services:** Align housing, homelessness and social services data to address root causes of crime and vulnerability.
- **Early intervention:** Leverage data on child welfare, school attendance, and family circumstances for timely support to at-risk families.
- **Performance monitoring:** Use comprehensive data to evaluate intervention effectiveness and drive continuous improvement.

3.2. Police opportunities

- **Crime pattern analysis:** Map hotspots using integrated data to identify patterns and target resources effectively.
- **Intelligence-led policing:** Enhance operational intelligence by drawing on cross-sector intelligence to disrupt criminal activity.
- **Risk assessment:** Access comprehensive information for more accurate risk evaluations.
- **Victim support:** Deliver more responsive, personalised care based on a holistic understanding of victims' needs.
- **Community engagement:** Respond to emerging community concerns through better-informed public engagement strategies.

3.3. Health sector opportunities

- **Mental health and substance misuse:** Coordinate care for individuals with complex needs across criminal justice and healthcare systems.
- **Trauma-informed care:** Use shared information on adverse childhood experiences to inform appropriate interventions.
- **Health inequalities:** Target resources to address social determinants that contribute to both poor health and crime.
- **Domestic violence and child safeguarding:** Improve collaboration to protect vulnerable individuals.
- **Health and justice:** Address the unmet health needs of offenders to improve rehabilitation and reduce reoffending.

3.4. Education sector opportunities

- **Early identification of need:** Identify at-risk students sooner through shared data with health, social care and community safety partners.
- **Alternative education provision:** Develop targeted interventions based on evidence.
- **School-based mental health support:** Enable timely, joined-up interventions between schools and health providers.
- **Bullying and safeguarding:** Improve detection and response to bullying or abuse through better information flows.
- **Post-school transition support:** Support young people as they move into adulthood, employment or further education with tailored, data-informed guidance.

3.5. Youth justice, probation, and prison services opportunities

- **Risk and needs assessment:** Use integrated data to develop more accurate risk profiles and tailored intervention plans.
- **Rehabilitation programming:** Design evidence-based interventions informed by multi-agency information.
- **Transition management:** Ensure continuity of support as individuals move between services.
- **Reoffending reduction:** Target resources towards individuals and areas with highest risk factors.
- **Family support:** Coordinate interventions that strengthen family support networks.

4

Recommendations and proposed approach for effective multi-agency data sharing



4

Recommendations and proposed approach for effective multi agency data sharing

Technology is a vital enabler of multi-agency collaboration, but it is not, on its own, the solution. The UK's persistent challenges in information sharing cannot be solved by infrastructure alone. The management of data requires a holistic operating model, comprising people, process and supporting technology. What's needed is a comprehensive, joined-up approach that aligns modern technology with governance, ethical frameworks, and trusted partnerships across sectors.

The shift must be from reactive response using disparate formats (emails, spreadsheets etc), to the establishment of partnership MADS capabilities able to support incident-driven data exchange to drive proactive, preventative information sharing. That means enabling practitioners to spot risk patterns early, intervene sooner, and work more effectively across organisational boundaries. This section outlines a practical, evidence-informed framework built around three interconnected pillars:



4.1. Technology foundations: Enabling secure, scalable and preventative data sharing

To underpin effective data sharing, public agencies need digital infrastructure that is secure, interoperable, and built for collaboration. Cloud-based architecture offers the most viable and future-proof foundation. Unlike traditional on-premise systems that have contributed to siloed data and slow responses, cloud platforms support real-time access, flexible scaling, and the secure integration of multiple data sources.

With cloud-based solutions:

- Near real-time access allows frontline professionals to view and act on up-to-date information, regardless of location - critical for timely safeguarding decisions.
- Shared infrastructure reduces duplication, lowers cost, and supports consistent, rapid deployment, especially important in resource-constrained public services.

Modern deployment methodologies such as Infrastructure as Code (IaC) streamline implementation by automating system configuration, ensuring consistent builds across agencies, and significantly reducing delivery timelines.

What once took months can now take weeks - crucial when addressing risks identified in serious case reviews.

Security is non-negotiable. A robust multi-agency solution must embed:

- End-to-end encryption of data in transit and at rest.
- Granular, role-based access controls aligned to professional responsibilities.
- Comprehensive audit trails to track access and ensure transparency.
- Active monitoring and threat detection to respond to potential breaches in near real-time.
- Data residency assurances to comply with UK legal and jurisdictional requirements.

By combining these technical capabilities, agencies can move toward a smarter, more secure model of information sharing - one that supports early intervention, builds trust, and enables real-world safeguarding outcomes.

4.2. Governance and data ethics

4.2.1. Information governance frameworks for preventive sharing

Robust governance frameworks provide the foundation for effective, appropriate, and legally compliant information sharing. They must balance the need to share information for safeguarding with the obligation to protect privacy and confidentiality. Crucially, these frameworks should support preventive information sharing to identify risk patterns early, rather than only after serious incidents. This requires fundamentally reorienting governance approaches to emphasise early risk identification while maintaining safeguards.

Clear information sharing protocols are vital, providing guidance on what can be shared, with whom, under what circumstances, and for what purposes. These protocols should establish lower thresholds for preventive sharing when patterns of concern are emerging and articulate legal gateways for different contexts, drawing on relevant legislation such as the Children Act 2004, the Care Act 2014, and the Police, Crime, Sentencing and Courts Act 2022. They should set clear thresholds for sharing information at different risk levels, addressing professional uncertainty identified as a barrier in serious case reviews, and shifting safeguarding practice from reactive to preventive.

Data controllership must be clearly defined within governance frameworks. Joint controller arrangements may suit multi-agency systems, with specific responsibilities allocated to each participating organisation. These arrangements should delineate accountability for data processing aspects, including quality assurance, subject access requests, and breach management.

Formal data sharing agreements between participating agencies provide the foundation for collaborative information exchange. They should cover all aspects of the relationship, including roles and responsibilities, data quality standards, dispute resolution, liability, termination provisions, and data handling if an agency withdraws from the collaboration.

Regular governance reviews ensure frameworks stay relevant as legislation, policy, and operational needs evolve. These reviews should involve all participating agencies and include feedback from frontline practitioners on governance application.

4.2.2. Data protection impact assessments and privacy by design

Data Protection Impact Assessments (DPIAs) are critical to identifying and mitigating privacy risks associated in multi-agency information sharing initiatives. These assessments should be conducted collaboratively, involving all relevant agencies, and revisited regularly as systems and processes evolve. DPIAs must cover the full information lifecycle, from collection and processing to storage, sharing, and deletion, and should establish clear ownership of risk mitigation actions.

Privacy by design principles should be embedded throughout the development and implementation of multi-agency data sharing solutions. This approach ensures that privacy considerations are addressed proactively rather than retrospectively, reducing the risk of costly remediation or regulatory intervention.

Key privacy by design elements include data minimisation (only collecting and sharing what is necessary), purpose limitation (using information only for clearly defined purposes), and storage limitation (retaining data only for as long as required). Technical measures such as pseudonymisation and encryption should be implemented where appropriate to provide additional privacy protections while enabling necessary information sharing.

Transparency is critical. All systems must provide clear, accessible privacy notices that explain how information is shared, under what legal basis, and what rights individuals have. These notices should be accessible to all service users, including those with additional needs or vulnerabilities.

4.2.3. Ethical decision-making frameworks

In complex safeguarding environments, legal compliance alone is not enough. Ethical decision-making frameworks are needed to guide professionals through situations where competing values - such as safety, autonomy, and confidentiality - must be balanced. These frameworks should be grounded in well-established ethical principles including beneficence, non-maleficence, justice, proportionality, and respect for autonomy.

Scenario-based guidance can help illustrate the application of ethical principles in real-world situations, building professional confidence in making appropriate sharing decisions. These resources should draw on lessons from serious case reviews, highlighting how ethical information sharing could have prevented negative outcomes.

Regular ethics forums bring together professionals from different agencies to discuss challenging cases and emerging issues, fostering a shared understanding of ethical approaches to information sharing. These forums can also identify areas where additional guidance or policy development is needed.

Independent ethical oversight, potentially through multi-agency ethics committees, provides assurance that information sharing practices remain aligned with societal values and expectations. These committees can review policies, procedures, and significant decisions, offering recommendations for improvement where appropriate.

4.3. Data partnerships

4.3.1. Stakeholder engagement and buy-in

Successful multi-agency data sharing depends fundamentally on effective partnerships between all organisations holding relevant information. Technical excellence and robust governance frameworks are necessary but insufficient without genuine commitment from all stakeholders.

Comprehensive stakeholder mapping should identify all organisations and individuals with an interest in the information sharing initiative, including their specific concerns, priorities, and potential contributions. This understanding enables tailored engagement strategies that address the particular needs and motivations of each stakeholder group.

Senior leadership engagement across all participating agencies is essential for establishing and maintaining effective data partnerships. Executive-level forums bring together leaders from different organisations to develop shared vision and strategy, allocate resources, and resolve cross-organisational challenges. These forums should establish clear accountability for delivery and demonstrate visible commitment to the collaborative approach.

Middle management also plays a key role in translating strategy into practice. Operational working groups can develop procedures, coordinate delivery, and ensure consistency across agencies. Equally important is the engagement of frontline practitioners, whose insights into day-to-day realities are essential for designing systems that work in practice. Practitioner reference groups should be maintained throughout implementation to support ongoing improvement.

The perspectives of service users must also be central. Advisory groups involving people with lived experience can help shape more respectful, transparent, and effective information-sharing approaches that maintain trust while meeting safeguarding objectives.

4.3.2. Building a culture of preventive information sharing

Culture change is essential to shift the emphasis from reactive to preventive data sharing. Professionals must be supported to move beyond defensive practices shaped by fear of sharing inappropriately. Serious case reviews have repeatedly identified professional anxiety as a key barrier to timely information sharing.

Addressing this anxiety requires a combination of clear guidance, supportive leadership, and opportunities for reflective practice that emphasise the value of preventive sharing. Decision support tools can help professionals navigate complex sharing decisions with a focus on early intervention, while regular case reviews should examine not only cases where harm occurred but also “near misses” where early information sharing successfully prevented escalation.

Leadership behaviours play a central role. Leaders at all levels should model appropriate information sharing, encourage open dialogue, and recognise positive practice. They should create psychological safety that enables professionals to raise concerns and seek guidance without fear of blame or criticism.

Celebrating success stories, where early data sharing prevented harm, helps build trust and reinforces the benefits of a preventive approach. Such stories also provide practical examples that professionals can learn from and apply to their own practice, gradually shifting the cultural emphasis from reactive to preventive information sharing.

Communities of practice offer a valuable forum for cross-agency dialogue, learning, and problem solving. These networks foster a collective approach to information sharing that transcends organisational boundaries and builds a shared professional identity focused on safeguarding.

Cultural change requires sustained effort. Change programmes must be based on a clear understanding of current attitudes and practices within each organisation and should be maintained over time to embed new behaviours and expectations.

4.3.3. Sustainable partnership governance

Long-term success requires sustainable partnership arrangements that can evolve in response to changing needs and circumstances. Formal partnership structures provide the foundation for this sustainability, with clear terms of reference, decision-making processes, and resource commitments.

Joint investment models ensure that all participating agencies contribute appropriately to the development and maintenance of shared information systems. These models should reflect both the benefits received and the capacity to contribute, with transparent formulas that all partners perceive as fair and equitable.

Performance management frameworks monitor not only technical system performance but also the effectiveness of information sharing in achieving desired outcomes. Regular reporting against agreed metrics enables early identification of issues and informed decision-making about future developments.

Dispute resolution mechanisms should be in place to handle disagreements constructively and preserve collaboration. These processes should include clear escalation pathways to senior forums when necessary.

Partnership review cycles provide a structured opportunity to reflect on progress, surface challenges, and realign objectives. All partners should be engaged in these reviews to ensure continued relevance and shared accountability.

By addressing technology, governance and data ethics, and data partnerships in a comprehensive, integrated manner, agencies can overcome the persistent challenges that have historically impeded effective information sharing.

This holistic approach recognises that successful multi-agency data sharing depends not only on technical solutions but also on the people, processes, and relationships that enable them to deliver their intended benefits.

5

Benefits of multi-agency data sharing



5

Benefits of multi-agency data sharing

The implementation of multi-agency data sharing (MADS) solutions represents a step-change in how public services approach safeguarding and community safety. Rather than focusing on isolated technical improvements, MADS delivers integrated, systemic change – bridging organisational boundaries and enabling earlier, smarter intervention. The benefits are both technical and operational, supporting a transition from reactive case management to proactive risk prevention.

5.1. Improved public safety and safeguarding

The most significant benefit of MADS lies in its capacity to transform safeguarding from a reactive exercise, often initiated after harm has occurred, to a preventive practice that identifies and addresses risks before they escalate.

Many tragic cases, from Victoria Climbié to Arthur Labinjo-Hughes, show how fragmented systems create blind spots that allow harm to go unnoticed. MADS helps solve this by connecting agencies, making risks clearer and enabling early intervention. The Radubukana case in Southport (2024) showed how separate data, if shared, could have revealed a pattern of concern. Beyond individual cases, MADS also helps identify wider trends, vulnerable communities, and service gaps, guiding smarter resource allocation and prevention strategies. By bringing information together, it transforms isolated data into meaningful intelligence, strengthening safeguarding efforts before crises emerge.

By transforming safeguarding from a reactive to a preventive practice, MADS supports key national strategies, including the National Data Strategy, Digital Strategy, and Police Science and Technology Strategy. It helps authorities meet their statutory obligations under the Serious Violence Duty, which mandates collaboration and data analysis for violence prevention. This alignment can unlock transformation funding and national programmes, providing resources for implementation. MADS also exemplifies digital transformation across agencies, reinforcing modernisation and evidence-based practice.

5.2. Service digital modernisation: Leveraging technology without major infrastructure upgrades

The technical architecture underpinning MADS delivers specific benefits that address long-standing barriers to effective information sharing. These technical advantages create the foundation upon which improved safeguarding practice can be built.

Modern MADS solutions fundamentally resolve the problem of delayed information transfer that has contributed to numerous safeguarding failures. By providing immediate access to crucial information across agency boundaries, these systems eliminate the dangerous delays that have historically hampered timely intervention.

This pragmatic approach recognises the complex IT landscape across the public sector and offers a path to integration that accommodates varying levels of technical maturity.

Cloud-based deployment models provide flexibility and scalability while reducing implementation complexity through Infrastructure as Code (IaC) methodologies. This approach delivers significant technical advantages, as illustrated in Table 5.2.

Table 5.2: Technical architecture benefits

Technical feature	Benefit to safeguarding practice
Near real-time data access	Eliminates delays in accessing critical information during risk assessment
Cloud infrastructure	Provides accessibility for mobile and remote workers making safeguarding decisions
Infrastructure as Code	Reduces implementation timeframes from months to weeks, accelerating benefit realisation
Scalable architecture	Accommodates growing data volumes and expanding user bases without service degradation
Standards-based exchange	Ensures consistent interpretation of information across professional contexts
Automated alerting	Notifies professionals when combined risk factors breach predetermined thresholds
Temporal analysis capabilities	Identifies patterns in risk factors over time, supporting nuanced understanding

5.3. Compliance and security: Ensuring data privacy, security, and ethics

Information sharing for safeguarding purposes must balance accessibility with robust protection for sensitive personal data. MADS solutions implement sophisticated security architecture that enables appropriate sharing while maintaining comprehensive safeguards.

Granular role-based access controls ensure users can only access information relevant to their professional responsibilities, implementing the principle of least privilege while enabling necessary information exchange. Comprehensive audit capabilities create tamper-proof records of all system activities, building accountability and supporting professional confidence in sharing decisions.

The security framework incorporates encryption for data both in transit and at rest, with specific attention to handling different security classifications appropriately. These technical measures directly support compliance with data protection legislation while enabling the information sharing essential for effective safeguarding.

5.3.1. Data management and quality enhancement

The persistent challenges in multi-agency information sharing often stem from inconsistent data quality and incompatible formats across different systems. MADS addresses these challenges through standardised data models, consistent terminology, and integrated quality management functions.

By establishing common data standards across participating agencies, MADS eliminates the variability that has historically hindered effective communication between professionals from different disciplines. Validation rules ensure completeness and accuracy during data entry, while automated cross-referencing can identify potential inconsistencies for resolution.

The system supports sophisticated data lifecycle management, including automated application of retention policies and efficient handling of subject access requests.

These capabilities ensure compliant data management while reducing the administrative burden on frontline services.

5.4. Operational efficiency and economic improvements of public services

While technical capabilities form the foundation of MADS, the most profound benefits emerge from how these systems transform professional practice, organisational cultures, and collaborative relationships enhancing operational efficiency. These non-technical benefits address the human and organisational factors that have persistently undermined effective information sharing.

5.4.1. Enhanced professional practice and decision-making

Access to comprehensive, timely information fundamentally enhances professional judgment in safeguarding contexts. MADS supports practitioners in making more informed decisions by providing visibility of the complete picture surrounding a vulnerable individual or family.

The system addresses the professional anxiety about sharing decisions that has frequently been identified as a barrier in serious case reviews. Clear governance frameworks, explicit thresholds, and comprehensive audit trails provide the structural support that enables professionals to share information with confidence in their legal and ethical position.

Standardised risk assessment frameworks ensure consistent evaluation across different professional contexts, reducing the variability that has undermined effective safeguarding. These frameworks support a shared understanding of risk while respecting the distinct perspectives that different disciplines bring to safeguarding practice.

5.4.2. Organisational efficiency and resource optimisation

Beyond enhancing safeguarding outcomes, MADS delivers substantial organisational benefits through improved efficiency and resource optimisation. These benefits are particularly significant in the current fiscal environment, where public services face increasing demand with constrained resources.

Reducing duplicate data entry saves time across agencies, as information entered once is accessible where needed. Streamlined referral processes and automated workflows cut administrative tasks, freeing up time for direct work with service users. Virtual collaboration and digital case file management reduce costs and inefficiencies, supporting flexible working arrangements.

Perhaps most significantly, data-driven insights enable more precise allocation of limited resources to areas of greatest need. This targeting ensures maximum impact from available resources while identifying opportunities for preventive intervention that may yield substantial long-term savings.

5.4.3. Economic benefits

The comprehensive benefits of MADS translate into substantial economic value through both efficiency gains and improved outcomes. These economic benefits support the business case for investment while demonstrating alignment with strategic priorities at local and national levels. It includes:

- Reduced costs through streamlined procedures and eliminated duplication.
- Decreased expenses through virtual collaboration capabilities.
- Lower technology costs through shared platforms and reduced duplication.
- Optimised deployment of specialist resources based on comprehensive data.
- Reduced crisis response costs through timely preventive action.
- More efficient use of professional time through improved information access.
- Reduction in routine administrative tasks through process automation.
- Decreased physical storage costs and associated administrative overhead.
- More efficient processing of inter-agency referrals through standardised digital pathways.

5.4.4. Cultural transformation and collaborative relationships

The deep-rooted cultural barriers to information sharing have proven remarkably resistant to change, despite numerous policy initiatives and tragic cases highlighting their consequences. MADS offers a catalyst for genuine cultural transformation by embedding new ways of working that gradually shift organisational norms and values.

Seeing the impact of effective information sharing builds momentum for change, creating cycles of better practice. As professionals experience its benefits, resistance fades and collaboration becomes the norm. Shared systems foster cross-agency dialogue, shaping collective wisdom and shifting risk-averse cultures. When leaders engage with system data, they reinforce safeguarding as a priority, setting clear expectations and driving lasting cultural change.

Integrated benefits matrix

Challenge domain	Technical benefits	Non-technical benefits
Information access	Near real-time data visibility across agencies	Enhanced decision-making through comprehensive information
Data quality	Standardised formats and validation rules	Consistent understanding across professional boundaries
Information security	Granular access controls and encryption	Professional confidence in appropriate sharing
Risk assessment	Automated alerting for combined risk factors	Standardised frameworks for consistent evaluation
Professional anxiety	Comprehensive audit trails and governance	Cultural shift towards preventive information sharing
Resource allocation	Data-driven insights and analytics	More effective targeting of limited resources
Collaborative working	Virtual spaces for multi-agency interaction	Strengthened relationships across organisational boundaries
Preventive practice	Pattern recognition across data sources	Shift from reactive to preventive intervention
Strategic planning	Aggregate data analysis and trend identification	Evidence-based commissioning and service development

The implementation of multi-agency data sharing (MADS) capability represents more than a technical improvement; it enables a fundamental shift from reactive to preventive approaches in safeguarding. By addressing persistent challenges identified in serious case reviews and delivering substantial operational efficiencies, MADS offers a transformative opportunity to improve outcomes for vulnerable individuals while optimising resource utilisation across partner agencies.

The integration of technical capabilities with practice enhancements and cultural change creates a powerful catalyst for system-wide improvement. While the technical infrastructure provides the foundation, the most profound benefits emerge from how these systems transform professional relationships, decision-making processes, and organisational cultures.

However, realising these benefits requires more than technical implementation - it demands coordinated attention to governance, leadership, and partnership development. The following section will outline an implementation framework that addresses these dimensions to ensure successful adoption and sustained value from MADS capability.

6

Implementation plan and options



6

Implementation plan and options

The significant benefits of multi-agency data sharing (MADS) identified in the previous section can only be realised through careful, systematic implementation that addresses technical, governance, and cultural dimensions simultaneously. This section presents a comprehensive implementation framework and action plan designed to guide organisations through the complex journey of establishing effective information sharing across agency boundaries.

6.1. Implementation approach

6.1.1. Principles for successful implementation

Successful MADS implementation requires adherence to several core principles that have emerged from both historical failures and positive case examples:

- **Evolutionary rather than revolutionary change:** Experience demonstrates that phased implementation yields more sustainable results than “big bang” approaches. By establishing initial capabilities that deliver early benefits whilst creating foundations for more advanced functionality, organisations build momentum and stakeholder confidence.
- **Co-design with practitioners:** Systems designed without meaningful frontline involvement typically fail to address operational realities and face adoption challenges. Implementation must involve those who will use the system daily in all stages of design and deployment.
- **Balanced focus across technology, process, and culture:** Technical excellence alone cannot overcome procedural complexity or cultural resistance. Implementation must address all three dimensions with equal rigour.
- **Evidence-based decision making:** Implementation decisions should be guided by evidence from both existing research and ongoing evaluation of the local implementation. This approach supports continuous refinement based on emerging learning.
- **Clear governance and accountability:** Effective implementations establish transparent decision-making structures with explicit accountability for delivery at executive, programme, and operational levels.

6.1.2. Phased implementation model

A four-phase implementation model provides a structured approach that balances early delivery of benefits with sustainable long-term development:

Phase 1: Foundation building (3 months)—Focus on establishing governance structures, legal frameworks, and core technical infrastructure whilst building stakeholder engagement.

Phase 2: Initial capability deployment (6 months)—Implement priority information sharing capabilities addressing the most critical safeguarding needs identified by frontline practitioners.

Phase 3: Expanded functionality (9-12 months)—Extend capabilities to additional agencies and information domains, incorporating learning from initial deployment.

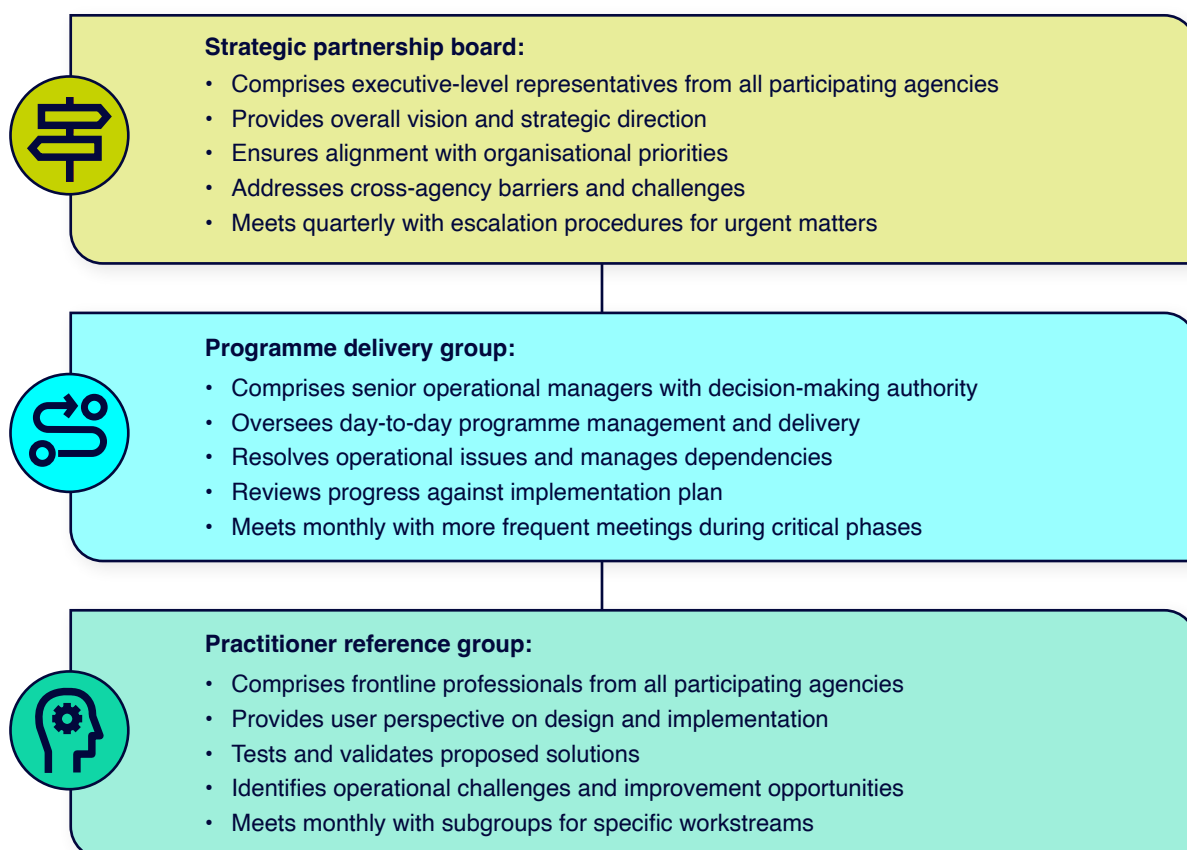
Phase 4: Advanced analytics and prevention (12+ months)—Develop sophisticated pattern recognition and forecasting capabilities to support increasingly preventive approaches.

This phased model recognises that MADS implementation represents a journey of continuous improvement rather than a finite project with a fixed endpoint.

6.2. Governance and programme structure

6.2.1. Multi-agency governance framework

Effective governance provides the foundation for successful implementation by ensuring clear decision-making, managing risks, and maintaining stakeholder engagement. A three-tier governance structure is recommended:



6.3. Technical implementation plan

6.3.1. Infrastructure deployment

The technical implementation begins with establishing the secure cloud infrastructure that will support MADS.

6.3.2. Data integration and application development

With the infrastructure in place, focus shifts to data integration and application development.

6.3.3. Security and compliance implementation

Security and compliance measures are integrated throughout the technical implementation, e.g.:

- Role-based access control systems aligned to information sharing agreements.
- Comprehensive audit logging and monitoring.
- Data encryption both in transit and at rest.
- Privacy-enhancing technologies such as pseudonymisation where appropriate,
- Automated compliance checking against governance frameworks.
- Regular security testing and vulnerability management.

6.4. Information governance implementation

6.4.1. Legal framework development

The information governance workstream establishes the legal and policy foundation for appropriate information sharing.

6.4.2. Policy and procedure development

With legal frameworks established, focus shifts to developing the operational policies needed for effective implementation.

6.5. Change management and adoption

6.5.1. Stakeholder engagement strategy

Effective stakeholder engagement is critical for overcoming the cultural barriers to information sharing.

6.5.2. Training and development programme

Comprehensive training ensures users can effectively utilise MADS capabilities.

6.6. Benefits realisation and evaluation

A structured approach to benefits measurement ensures the programme delivers meaningful improvements.

6.7. Critical success factors

Based on experience from successful MADS implementations and lessons from historical challenges, several factors are critical to success:

- I. **Unwavering senior leadership commitment:** Active, visible sponsorship from the most senior leaders in each participating agency, maintained throughout the implementation journey.
- II. **Genuine multi-agency ownership:** Shared responsibility for success rather than domination by a single agency, reflected in governance structures and resource contributions.
- III. **Frontline practitioner involvement:** Meaningful engagement of those who will use the system daily, from initial requirements through to evaluation.
- IV. **Balanced focus on technology, process, and culture:** Equal attention to all three dimensions rather than treating MADS as primarily a technical implementation.
- V. **Pragmatic, phased approach:** Delivering tangible benefits incrementally rather than attempting comprehensive transformation in a single step.
- VI. **Clear connection to safeguarding outcomes:** Maintaining focus on improved outcomes for vulnerable individuals rather than system implementation for its own sake.
- VII. **Dedicated resources with appropriate skills:** Ensuring the programme is properly resourced with the right expertise across all workstreams.
- VIII. **Learning orientation:** Commitment to continuous learning and adaptation based on implementation experience and emerging challenges.

6.8. Self-managed implementation or in partnership with Capita

The implementation roadmap described above provides a comprehensive framework for organisations pursuing self-managed MADS deployments. However, to significantly reduce technical complexity of implementation, accelerate timeline, mitigate risks, minimise technical burden on participating agencies, provide cost-effective scaling and continuous improvement and innovation, collaborating with an experienced partner can be a better option.

Aiming to help multiple government agencies share important data collectively to enhance public protection Capita offers a fully hosted managed service for MADS capability implementation. Our solution was developed in direct response to the data sharing challenges and the requirements of the Serious Violence Duty.

Our multi-agency data sharing technical solutions team and Centre of Excellence provide comprehensive support across all aspects of MADS implementation, addressing the complexity and challenges outlined above. This support includes:

6.8.1. Technical implementation services

We offer a complete technical solution built on Microsoft Fabric, with pre-configured components that significantly accelerate implementation:

- Cloud infrastructure templates using Infrastructure as Code methodologies.
- Efficient, secure and standardised process of ingesting source data.
- Configurable data to support insights such as event cost analysis.
- Comprehensive security architecture compliant with UK standards.
- Flexible deployment options accommodating different agency requirements.

These technical assets typically reduce implementation timeframes by 40-50% compared to custom-built solutions, while providing greater reliability and security.

6.8.2. Information governance support

The Centre of Excellence for Data Sharing provides extensive governance expertise:

- Template information sharing agreements and protocols.
- Pre-completed Data Protection Impact Assessments adaptable to local contexts.
- Decision support frameworks for operational information sharing.
- Policy templates covering all aspects of information governance.
- Specialist advice on complex legal and ethical questions.

This governance support addresses one of the most challenging aspects of the MADS capability implementation, providing confidence in the legal basis for appropriate information sharing.

6.8.3. Change management and adoption services

Our implementation methodology incorporates comprehensive change support:

- Stakeholder engagement frameworks and communication templates.
- Training materials and delivery methodologies.
- Cultural assessment tools and intervention approaches.
- Benefits tracking and realisation methodologies.
- Adoption measurement and improvement techniques.



These resources draw on experience from successful implementations across multiple sectors, addressing the cultural and behavioural aspects that often determine success.

6.8.4. Partnership approach

Recognising that successful MADS implementation requires genuine partnership, we offer flexible engagement models:

- Knowledge transfer to build local capability alongside direct delivery.
- Skills development for in-house teams to support long-term sustainability.
- Phased transition from supported to self-sufficient operation.
- Ongoing access to expertise from the Centre of Excellence.

This approach ensures that implementing organisations develop the internal capabilities needed for sustainable operation while benefiting from Capita's extensive experience in multi-agency information sharing.

6.8.5. Benefits of MADS capability implementation with Capita

Our MADS capability provides a complete end-to-end technical and operational environment for secure, multi-agency data sharing, which includes:

- Secure cloud infrastructure.
- Pre-configured MADS platform.
- Integration services.
- Managed technical operations.
- Comprehensive support services.

The implementation of MADS capability with us brings substantial benefits to safeguarding partnerships.

Benefit category	Capita MADS capability advantages
Implementation timeline	<ul style="list-style-type: none"> • Typical reduction of 6-9 months in time to initial capability • Elimination of lengthy procurement and design phases • Accelerated configuration vs. custom development • Rapid scaling to additional agencies and users
Technical complexity	<ul style="list-style-type: none"> • Elimination of infrastructure design and deployment challenges • Reduced integration complexity through efficient, secure and standardised processes for ingesting source data • Comprehensive security management by specialists • Simplified technical architecture and operations
Resource requirements	<ul style="list-style-type: none"> • Significantly reduced technical staffing needs • Less demand on agency IT departments • Rebalanced focus towards practice and governance • Access to specialist expertise without recruitment
Economic value	<ul style="list-style-type: none"> • Reduction in total cost of ownership over 5 years • Conversion of capital to operational expenditure • Earlier realisation of efficiency benefits • Predictable costs without technical refresh spikes
Risk profile	<ul style="list-style-type: none"> • Reduced technical delivery risk through proven platform • Enhanced security through specialist management • Lower dependency on scarce technical skills • Greater predictability in timelines and costs
Strategic focus	<ul style="list-style-type: none"> • Increased emphasis on practice and culture vs. technology • Enhanced governance support and expertise • Knowledge transfer from multiple implementations • Continuous improvement without major reinvestment
Safeguarding impact	<ul style="list-style-type: none"> • Earlier risk identification through accelerated implementation • More timely interventions to prevent harm • Reduced opportunity cost of delayed capabilities • Continuous enhancement of preventive capabilities

7

From possibility to practice



7

From possibility to practice

Despite the lessons of countless serious case reviews, effective multi-agency information sharing remains one of the most persistent challenges in safeguarding. Fragmented systems, legal uncertainty, cultural hesitation, and inconsistent practice continue to undermine the protection of vulnerable individuals, often with tragic consequences.

From Victoria Climbié to Arthur Labinjo-Hughes and more recent cases such as Radubukana in Southport, the pattern is painfully clear: information is not shared efficiently. Siloed systems, inconsistent risk frameworks, and professional uncertainty create gaps where harm can escalate unseen.

This white paper has explored how a more integrated, preventive approach to information sharing can transform not just systems, but outcomes. Multi-agency data sharing (MADS) capability offers a comprehensive and practical response to these entrenched challenges. By enabling near real-time information access, standardised risk assessment, and improved data quality, MADS supports earlier identification of need, more consistent decision-making, and more coordinated safeguarding responses.

But technology alone will not drive this change. It must be underpinned by clear governance, professional trust, cultural alignment, and sustained leadership. MADS can provide the infrastructure, but people, partnerships, and purpose will ultimately determine its impact.

The question now is not whether we can share information more effectively, but whether we will.

Enabling change and action

To support progress across sectors, we invite organisations to consider the following:

- 1) Reflect on local lessons**
What have recent cases or reviews shown about information-sharing gaps in your area?
- 2) Start small, but start now**
Identify one critical area, such as domestic abuse, serious violence, or children's safeguarding, where earlier, joined-up data could make a difference.
- 3) Engage practitioners early**
Frontline professionals must help shape any new approach if it's to work in practice.
- 4) Build on what exists**
MADS is about connection, not replacement. Start from your current systems, relationships, and successes.
- 5) Commit to shared leadership**
Information sharing is everyone's responsibility, but it needs champions.

Next steps

If your organisation is exploring how to improve data sharing across agencies or partnerships, we welcome the opportunity to share insights, case studies, and approaches that have worked successfully.

To learn more about our MADS capability or to connect with our team, visit content.capita.com/MADS or e-mail bettergovernment@capita.com.



References

1. **Laming, H. (2003).** The Victoria Climbié Inquiry. London: HMSO. Available at: <https://www.gov.uk/government/publications/the-victoria-climbié-inquiry-report-of-an-inquiry-by-lord-laming>
2. **Department for Education. (2023).** Working Together to Safeguard Children. London: HMSO. Available at: https://assets.publishing.service.gov.uk/media/669e7501ab418ab055592a7b/Working_together_to_safeguard_children_2023.pdf
3. **Information Commissioner's Office. (2024).** Data Sharing Code of Practice. Wilmslow: ICO. Available at: <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-sharing/data-sharing-a-code-of-practice/>
4. **National Police Chiefs' Council. (2020).** National Policing Digital Strategy 2020-2030. London: NPCC. Available at: <https://pds.police.uk/wp-content/uploads/2020/01/National-Policing-Digital-Strategy-2020-2030.pdf>
5. **HM Government. (2022).** National Data Strategy. London: HMSO. Available at: <https://www.gov.uk/guidance/national-data-strategy>
6. **Child Safeguarding Practice Review Panel. (2022).** National Review into the murders of Arthur Labinjo-Hughes and Star Hobson. London: HMSO. Available at: <https://www.gov.uk/government/publications/national-review-into-the-murders-of-arthur-labinjo-hughes-and-star-hobson>
7. **Home Office. (2023).** Serious Violence Duty Statutory Guidance. London: HMSO. Available at: <https://www.gov.uk/government/publications/serious-violence-duty-non-statutory-guidance>
8. **UK Government. (2022).** UK Science and Technology Framework. London: HMSO. Available at: <https://www.gov.uk/government/publications/uk-science-and-technology-framework/the-uk-science-and-technology-framework>
9. **Home Office. (2022).** Police Science and Technology Strategy. London: HMSO. Available at: <https://science.police.uk/strategy/>
10. **Department of Health and Social Care. (2020).** Joined-up care: The Digital Health and Social Care Plan. London: HMSO. Available at: <https://www.gov.uk/government/publications/a-plan-for-digital-health-and-social-care>
11. **Information Commissioner's Office. (2024).** New ICO campaign promotes sharing data to safeguard children. Available at: <https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2024/01/new-ico-campaign-promotes-sharing-data-to-safeguard-children/>
12. **Home Office. (2024).** Prevent Learning Review: Southport Attack - Axel Muganwa Rudakubana. Available at: <https://www.gov.uk/government/publications/prevent-learning-review-southport-attack/prevent-learning-review-axel-muganwa-rudakubana-accessible>
13. **Local Government Information Unit. (2013).** Daniel Pelka Serious Case Review - Coventry LSCB. Available at: <https://lgiu.org/wp-content/uploads/2013/10/Daniel-Pelka-Serious-Case-Review-Coventry-LSCB.pdf>
14. **Department for Education. (2008).** Haringey Local Safeguarding Children Board: First Serious Case Review Child A. Available at: <https://www.gov.uk/government/publications/haringey-local-safeguarding-children-board-first-serious-case-review-child-a>
15. **Association of Police and Crime Commissioners. (2023).** About the Association, the Role and Responsibilities of PCCs. Available at: <https://www.apccs.police.uk/about-the-apcc/>

 Capita