SUAT Data Sharing Policy and Code of Practice

Last reviewed	**August 2025**
Reviewed by	**Operations Director**
Approved by	**Trust Board**
Date of approval	**August 2025**
Policy owner	**DPO**
Location	**Trust Website**

This policy is based on the ICO's Data Sharing Code of Practice made under section 121 of the Data Protection Act 2018, which is a practical guide for organisations about how to share personal data in compliance with data protection legislation. The ICO's Code of Practice explains the law and provides good practice recommendations, including that when sharing data, organisations must follow the UK GDPR's Data Protection Principles.

Data sharing can help public bodies to fulfil their functions and deliver modern, efficient services that make everyone's lives easier. It can help keep vulnerable individuals safe at times of crisis, produce official statistics, research and analysis for better decision-making for the public good. Conversely, not sharing data can mean that everyone fails to benefit from these opportunities; and in some instances, the chance is missed to assist people in need, whether in urgent or longer-term situations.

This policy's purpose is to support with the management of risks relating to data sharing. Data Controllers are defined under Article 4 of the UK GDPR and section 32 of the DPA 2018 as having responsibility for deciding the "purposes and means of the processing of personal data". The Trust and academies will share personal data in a way that is fair, transparent and in line with the rights and expectations of the people whose information is being shared. When sharing data, the Trust and academies are required to follow the key principles in data protection legislation, as defined in SUAT's Data Protection Policy.

The Trust and academies recognise the importance of timely and effective information sharing when safeguarding and promoting the welfare of pupils. It is important that all academies are clear on when information should be shared and how staff members should do this whilst understanding that the Data Protection Act 2018 and UK GDPR are not barriers to the sharing of information for the purposes of keeping children safe.

This policy has due regard to all relevant legislation and statutory guidance including, but not limited to, the following:

- ICO (2023) 'A 10 step guide to sharing information to safeguard children'
- DfE (2024) 'Keeping children safe in education 2024' (KCSIE)
- DfE (2024) 'Information sharing'
- UK GDPR
- Data Protection Act 2018
- DfE (2023) 'Working Together to Safeguard Children 2023'

1. Policy Aims

This policy aims to:

- Assure individuals whose data the Academies and Trust process;
- Provide confidence in our processing activities;
- Provide information regarding when it is appropriate to share personal data;
- Support employees in sharing data appropriately and compliantly;
- Provide employees with the confidence to share data in a one-off situation or in an emergency;
- Reduce reputational risks when sharing data;
- Provide more robust sharing practices and better protection for individuals whose data is shared;
- Demonstrate compliance with the law;
- Prevents harm and promotes the welfare of pupils.

2. Data Sharing Definitions

The scope of data sharing is defined by Section 121 of the Data Protection Act 2018 as “the disclosure of personal data by transmission, dissemination or otherwise making it available”. This includes:

- Providing personal data to a third party, by whatever means;
- Receiving personal data as a joint participant in a data sharing arrangement;
- The two-way transmission of personal data;
- Providing a third party with access to personal data on or via IT systems.

Information sharing in a safeguarding context means the appropriate and secure exchange of personal information, between staff and third-party organisations with a responsibility for children, in order to keep them safe from harm. This includes informal sharing of information between practitioners and professionals to develop an accurate understanding of a child or family.

Routine data sharing

This is data sharing done on a regular basis in a routine, pre-planned way. It generally involves sharing data between organisations for an established purpose.

Ad hoc or one-off data sharing

In some instances, data sharing may take place in ad hoc situations that are not covered by any routine arrangement. Sometimes data sharing may take place in conditions of real urgency, or even in an emergency situation. In an urgent situation, the risks should be assessed, to do what is necessary and proportionate.

Data pooling

Data pooling is a form of data sharing whereby organisations decide together to pool information they hold and make it available to each other, or to different organisations, for a specific purpose or purposes.

3. Responsibilities

In order to remain compliant with the UK GDPR and the information rights of data subjects, those handling data on behalf of the Academy / Trust will:

- Consider whether they should be accessing or disclosing personal data before they do so and ensure that they have appropriate authority to share the information.
- Be aware that, under the UK GDPR, they may be personally liable for any data disclosure.
- When transferring data to an individual or organisation, ensure they have appropriately verified that the individual or organisation are authorised to receive the data. To do this, a process for verifying the identity of the recipient will be used. Individuals will be made aware that by sharing data, they are taking personal responsibility for this process and may be required to justify their actions in the event of a complaint.
- Not discuss data held by the Academy/Trust with unauthorised colleagues, or family members, friends or other associates and stakeholders of the Academy/Trust community.

- Not access organisational records containing personal, sensitive or confidential data other than for a specified and legitimate purpose. Accessing personal data without a specified and legitimate purpose may lead to disciplinary action or be considered as a breach under data protection legislation.
- Avoid providing any specific details about individuals that might lead to their identification when using data for reports or monitoring purposes.
- Use the blind carbon copy (BCC) option when sending out the same email to a number of people to their personal email accounts (for example, parents) unless recipients have agreed to share their personal email addresses with others.
- Always consider data security and the risks associated with losing personal data, before processing, using, downloading, sharing, transporting or printing any personal data.
- Never share or write down passwords to systems where personal data is stored. Doing so could result in unauthorised access to personal data and, therefore, could constitute a serious security breach.
- Ensure their passwords related to data handling systems are created in line with the relevant data protection and information security policies.
- Always secure devices that hold data when they are left unattended – this includes logging out of devices or services at the end of the day or when they are no longer being used.
- Take adequate precautions to protect organisational data in a public place – this includes protecting any mobile devices, laptops or tablets that may contain data or have the ability to access data.
- Take immediate action in the event of a data breach and report any breaches using the process within the personal data breach management plan.
- Ensure that only the necessary data is shared. Where it is not necessary to share that data, under the data minimisation and purpose limitation principles, it must be redacted.
- Ensuring that data being shared is appropriately protected, whether verbally, in paper based or electronic forms, e.g. securing and encrypting emails, ensuring that verbal conversations are held in an appropriate location. Personal and sensitive data should not be shared on email in an unprotected format.
- Ensuring that the data they share is accurate and up to date.
- Ensuring that data is shared securely and managed in accordance with the Information Security Policy.

When sharing personal data, Academies must ensure:

- Staff have appropriately detailed advice about which datasets they can share, to prevent irrelevant or excessive information being disclosed.
- That the data they are sharing is accurate.
- Appropriate technical and organisational security arrangements are in place to protect personal information, including the transmission of the data.
- Procedures for identifying, reporting and managing any breach are followed in a timely manner.
- Staff are properly trained and are aware of their responsibilities for any shared data they have access to.
- The procedure for dealing with subject access requests is adhered to.

- There are procedures for dealing with the termination of the data sharing initiative, including the deletion of shared data or its return to the organisation that supplied it originally.
- That data is redacted or anonymised where necessary.

The Headteacher will be responsible for:

- The implementation of this policy.
- Ensuring staff receive appropriate and regular data protection and safeguarding training as required and at least annually.
- Implementing systems which enable staff to share safeguarding information without fear of breaking data protection law.

The LAC will be responsible for:

- Overseeing the policy's implementation.
- Holding the setting to account for its systems and processes for sharing safeguarding information and assessing their effectiveness.
- Ensuring staff have due regard to the relevant data protection principles enabling them to share and withhold personal information for safeguarding purposes.

The DSL will be responsible for:

- Being the first point of contact when safeguarding concerns and information needs to be reported.
- Providing guidance and support to staff members regarding the recognition and reporting of safeguarding concerns and information.
- Quality assuring training provision to ensure it is high quality and up to date.
- Being confident of processing conditions that enable them to store and share information required to carry out their safeguarding role.
- Undertaking in-depth training and CPD.

The DPO will be responsible for:

- Overseeing the implementation of DPIAs.
- Assessing risks associated with sharing safeguarding information in liaison with the DSL.
- Providing guidance and support to staff members regarding data protection legislation and sharing information appropriately.
- Making it clear to staff members that sharing information relating to pupils at risk of harm is not prevented by data protection law.

All staff will be responsible for:

- Reporting any known safeguarding information.
- Making themselves aware of data protection law and how it applies to the sharing of information relating to safeguarding.
- Participating in training and keeping up to date with relevant developments.
- Seeking advice from the DSL and DPO and DPL as appropriate.
- Reading any notices or emails regarding the sharing of safeguarding information and asking any questions as appropriate.
- Being alert to safeguarding concerns and indicators of abuse and neglect.

- Carrying forward disclosures of safeguarding issues by pupils to the DSL.

Parents will be responsible for:

- Cooperating with the academy where safeguarding information regarding their child is being shared.
- Reporting concerns regarding their child's wellbeing to the academy and that which concerns other pupils' wellbeing if appropriate.

4. Information Sharing Guidance

In accordance with the Government guidance on information sharing (link) the seven golden rules to sharing information are:

1. All children have a right to be protected from abuse and neglect. Protecting a child from such harm takes priority over protecting their privacy, or the privacy rights of the person(s) failing to protect them. The UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA) provide a framework to support information sharing where practitioners have reason to believe failure to share information may result in the child being at risk of harm.
2. When you have a safeguarding concern, wherever it is practicable and safe to do so, engage with the child and/or their carer(s), and explain who you intend to share information with, what information you will be sharing and why. You are not required to inform them, if you have reason to believe that doing so may put the child at increased risk of harm (e.g., because their carer(s) may harm the child, or react violently to anyone seeking to intervene, or because the child might withhold information or withdraw from services).
3. You do not need consent to share personal information about a child and/or members of their family if a child is at risk or there is a perceived risk of harm. You need a lawful basis to share information under data protection law, but when you intend to share information as part of action to safeguard a child at possible risk of harm, consent may not be an appropriate basis for sharing. It is good practice to ensure transparency about your decisions and seek to work cooperatively with a child and their carer(s) wherever possible. This means you should consider any objection the child or their carers may have to proposed information sharing, but you should consider overriding their objections if you believe sharing the information is necessary to protect the child from harm.
4. Seek advice promptly whenever you are uncertain or do not fully understand how the legal framework supports information sharing in a particular case. Do not leave a child at risk of harm because you have concerns you might be criticised for sharing information. Instead, find out who in your organisation/agency can provide advice about what information to share and with whom. This may be your manager/supervisor, the designated safeguarding children professional, the data protection/information governance lead (e.g., Data Protection Officer), Caldicott Guardian, or relevant policy or legal team.
5. When sharing information, ensure you and the person or agency/organisation that receives the information take steps to protect the identities of any individuals (e.g., the child, a carer, a neighbour, or a colleague) who might suffer harm if their details became known to an abuser or one of their associates.
6. Only share relevant and accurate information with individuals or agencies/organisations that have a role in safeguarding the child and/or providing

their family with support, and only share the information they need to support the provision of their services. Sharing information with a third party rarely requires you to share an entire record or case-file – you must only share information that is necessary, proportionate for the intended purpose, relevant, adequate and accurate.

7. Record the reasons for your information sharing decision, irrespective of whether or not you decide to share information. When another practitioner or organisation requests information from you, and you decide not to share it, be prepared to explain why you chose not to do so. Be willing to reconsider your decision if the requestor shares new information that might cause you to regard information you hold in a new light. When recording any decision, clearly set out the rationale and be prepared to explain your reasons if you are asked.

5. Sharing Personal Information

Data protection law requires organisations to process personal data securely, with appropriate organisational and technical measures in place. The security measures must be "appropriate" to the nature, scope, context and purpose of the processing and the risks posed to the rights and freedoms of individuals.

The sharing of personal data must be fair and in a transparent manner, to mitigate against unjustified adverse effects on the individual; sharing personal data must be reasonable and proportionate. As part of the fairness and transparency considerations, settings should also bear in mind ethical factors when deciding whether to share personal data and ask whether it is right to share it.

Organisations that data is shared with take on their own legal responsibilities for the data, including its security. Reasonable steps should be taken to ensure that the data shared will continue to be protected with adequate security by the recipient organisation. The recipient should understand the nature and sensitivity of the information; reasonable steps must be taken to be certain that security measures are in place, and any difficulties must be resolved before personal data is shared in cases where there are different standards of security, different IT systems and procedures, different protective marking systems etc. between the parties involved in the sharing.

When sharing the personal information of children, the best interests of the child is the primary consideration. Settings should not share personal data unless there is a compelling reason to do so, taking account of the best interests of the child. One clear example of a compelling reason is data sharing for safeguarding purposes; another is the importance for official national statistics of good quality information about children. Children are less aware than adults of the risks involved in having their data collected and processed, therefore the law says that organisations have a responsibility to assess the risks and put appropriate measures in place.

Urgent or emergency situations can arise that may not have been envisaged. In an emergency, Academies should share data as is necessary and proportionate; this may include preventing serious physical harm to a person; preventing loss of human life; protection of public health; safeguarding vulnerable adults or children; responding to an emergency; or an immediate need to protect national security.

When taking decisions about what information to share, staff should consider how much information they need to release. Not sharing more data than is necessary to be of use is a key element of the UK GDPR and Data Protection Act 2018, and staff should consider the

impact of disclosing information on the information subject and any third parties. Information must be proportionate to the need and level of risk and:

- Only information that is relevant to the purposes should be shared with those who need it. This allows others to do their job effectively and make appropriately informed decisions.
- Information should be adequate for its purpose and of the right quality to ensure that it can be understood and relied upon.
- Information should be accurate and up to date and should clearly distinguish between fact and opinion. If the information is historical then this should be explained.

Information must be shared in an appropriate, secure way. Academies must follow security measures as outlined the Data Protection, Retention and Records Management and Information Security policies, for handling personal information.

Information sharing decisions should be recorded and whether or not the decision is taken to share, under the data protection principle of accountability. If the decision is to share, reasons should be cited including what information has been shared and with whom, in line with Academy and Trust procedures. If the decision is not to share, it is good practice to record the reasons for this decision and discuss with any individuals requesting the data.

In line with the Retention and Records Management Policy and principle of storage limitation, information should not be kept any longer than is necessary. In some rare circumstances such as for historical and research purposes, this may be indefinitely, but if this is the case, there should be a review process scheduled at regular intervals to ensure data is not retained where it is unnecessary to do so. The DPO should be consulted.

Each time data is shared outside of the setting, a 'check and send' culture to ensure that the data being shared, and who is it being shared with, is logged appropriately, as good practice.

When asked to share information, staff should consider the following questions to help decide if, and when, to share. If the decision is taken to share, they should consider how best to effectively share the information.

Check whether the sharing is justified

Key points to consider:

☐ What is the sharing meant to achieve?

☐ Have you assessed the potential benefits and risks to individuals and/or society of sharing or not sharing?

☐ Is it fair to share data in this way?

☐ Is the sharing necessary and proportionate to the issue you are addressing?

☐ What is the minimum data you can share to achieve the aim?

☐ Could the objective be achieved without sharing personal data, or by sharing less personal data?

☐ What safeguards can you put in place to minimise the risks or potential adverse effects of the sharing?

☐ Is there an applicable exemption in the DPA 2018?

Consider doing a Data Protection Impact Assessment

Decide whether you need to carry out a DPIA:

☐ You must do a DPIA for data sharing that is likely to result in a high risk to individuals. This will depend on the nature, scope, context and purposes of the sharing.

☐ For any data sharing plans, you may find it useful to follow the DPIA process as a flexible and scalable tool to suit your project.

If you decide to share

It is good practice to have a data sharing agreement. As well as considering the key points above, your data sharing should cover the following issues.

☐ What information will you share?

☐ Is any of it special category data (or does it involve sensitive processing under Part 3 of the DPA 2018)? What additional safeguards will you have in place?

☐ How should you share the information?

- You must share information securely.
- You must ensure you are giving the information to the right recipient.

☐ What is to happen to the data at every stage?

☐ Who in each organisation can access the shared data? Ensure it is restricted to authorised personnel in each organisation.

☐ What organisation(s) will be involved? You all need to be clear about your respective roles.

☐ How will you comply with your transparency obligations?

- Consider what you need to tell people about sharing their data and how you will communicate that information in a way that is concise, transparent, easily accessible and uses clear and plain language.
- Consider whether you have obtained the personal data from a source other than the individual.
- Decide what arrangements need to be in place to comply with individuals' information rights. Bear in mind the differences under Part 3 of the DPA 2018, if applicable.

☐ What quality checks are appropriate to ensure the shared data is accurate and up-to-date?

☐ What technical and organisational measures are appropriate to ensure the security of the data?

☐ What common retention periods for data do you all agree to?

☐ What processes do you need to ensure secure deletion takes place?

☐ When should regularly scheduled reviews of the data sharing arrangement take place?

Accountability principle

You must comply with the principles; this point focuses on the accountability principle:

☐ The accountability principle means that you are responsible for your compliance with the UK GDPR or DPA 2018 as appropriate and you must be able to demonstrate that compliance.

☐ You must maintain documentation for all your data sharing operations.

☐ This obligation encompasses the requirement to carry out a DPIA when appropriate.

☐ You must implement a “data protection by design and default” approach, putting in appropriate technical and organisational measures to implement data protection principles and safeguard individual rights.

☐ You must ensure that staff in your organisation who are likely to make decisions about sharing data have received the right training to do so appropriately.

Decide what your lawful basis is for sharing the data

Key points to consider:

☐ What is the nature of the data and the purpose for sharing it, as well as the scope and context?

☐ Are you relying on legitimate interests as a lawful basis?

☐ Is any of the data either special category data or criminal offence data? If so, you need to identify additional conditions.

☐ For law enforcement processing under Part 3 of the DPA 2018, please refer to the references throughout the code and in particular to the Part 3 section.

Check whether you have the power to share

Key points to consider:

☐ What type of organisation you work for.

☐ Any relevant functions or powers of your organisation.

☐ The nature of the information you have been asked to share.

☐ Whether there are any legal requirements that need to be met when sharing the data - such as copyright or a duty of confidence, or any prohibitions.

☐ Whether there is a legal obligation or other legal requirement about sharing information – such as a statutory requirement, a court order or common law.

Document your decision

Document your data sharing decision and your reasoning – whether or not you share the information.

If you shared information you should document:

☐ your justification for sharing;

☐ what information was shared and for what purpose;

☐ who it was shared with;

☐ when and how it was shared;

☐ whether the information was shared with or without consent, and how that was recorded;

☐ the lawful basis for processing and any additional conditions applicable;

☐ individuals’ rights;

☐ Data protection impact assessment reports;

☐ compliance with any DPO advice given (where applicable);

☐ evidence of the steps you have taken to comply with the UK GDPR and the DPA 2018 as appropriate; and

☐ where you have reviewed and updated your accountability measures at appropriate intervals.

Staff will be reminded to follow the ‘think, check, share’ procedure when assessing whether it is necessary to share information:

- **Think** – Staff will consider the purpose of sharing the information and whether there is a legal basis to do so, consulting data leads and the DPO as necessary. Staff will consider the data that is needed to fulfil the purpose of the information sharing and how this can be minimised and protected.

- **Check** – Staff will consider who should be made aware of the information and how this can be communicated safely and securely.

- **Share** – Finally, staff will share the information with those who need to know so that.

The Data Protection Act 2018 balances the rights of the information subject (the individual whom the information is about) and the possible need to share information about them. It is essential to consider this balance in every case. Staff should always keep a record of what they have shared and if it is strictly necessary to share the information, any personal, confidential or sensitive information must be shared in a secure format e.g. via encrypted email.

Arrangements for sharing data with third parties should ensure that all parties:

- Have detailed advice about which datasets they can share, to prevent irrelevant or excessive information being disclosed;
- Make sure that the data they are sharing is accurate;
- Record data in the same format;
- Have common rules for the retention and deletion of shared data items, as appropriate to their nature and content, and procedures for dealing with cases where different organisations may have different statutory or professional retention or deletion rules;
- Have common technical and organisational security arrangements, including the transmission of the data and procedures for dealing with any breach of the agreement in a timely manner;
- Ensure their staff are properly trained and are aware of their responsibilities for any shared data they have access to;
- Have procedures for dealing with access requests, complaints or queries from members of the public;
- Have a timescale for assessing the ongoing effectiveness of the data sharing;
- Have procedures for dealing with the termination of the data sharing arrangement.

6. The Accountability Principle of the UK GDPR

The accountability principle means that organisations are responsible for their compliance with the UK GDPR or DPA 2018, and recording actions and decisions taken in relation to data protection matters, including:

- Maintaining documentation for all data sharing operations
- Sharing personal data fairly and transparently
- Ensuring that the basis for sharing the data is lawful
- Completing data protection impact assessments where necessary
- Ensuring that the sharing is authorised
- Providing appropriate training for staff who share personal information
- Ensuring any legal requirements are met when sharing the data - such as copyright or a duty of confidence, or any prohibitions
- Processing personal data securely, with appropriate organisational and technical measures in place

- Sharing data in an emergency, as is necessary and proportionate
- Taking account of the best interests of the child when sharing their personal data and ensuring that there is a legitimate reason to do so
- Ensuring data sharing agreements are in place where required
- Following the government devised framework for the sharing of personal data, for defined purposes across the public sector, under the Digital Economy Act 2017 (DEA).

For any information sharing, Academies should be able to document:

- The justification for sharing
- What information was shared and for what purpose
- Who it was shared with
- When and how it was shared
- Whether the information was shared with or without consent, and how consent was recorded
- The lawful basis for processing and any additional conditions applicable
- Individuals' rights
- Data protection impact assessments
- Compliance with any ICO or DPO advice given (where applicable)
- Evidence of the steps taken to comply with the UK GDPR and the DPA 2018 as appropriate
- Where accountability measures have been reviewed and updated at appropriate intervals

When thinking about sharing data, as well as considering whether there is a benefit to the data sharing and whether it is necessary, the academies and Trust must consider overall compliance with data protection legislation, including fairness and transparency. It is good practice to carry out a Data Protection Impact Assessment if there is a major project that involves disclosing personal data, or any plans for routine data sharing, even if there is no specific indicator of likely high risk. Data sharing that is likely to result in a high risk to individuals needs to be accompanied by a DPIA and will depend on the nature, scope, context and purposes of the sharing.

Each setting will keep in mind the principles of the UK GDPR, the Data Protection Act 2018 and human rights law as frameworks to ensure that information is shared appropriately. Staff will be provided with information on where they can receive advice on data protection in order to make the right decisions when sharing information.

The following data protection principles must be adhered to when sharing information:

- Lawfulness, fairness and transparency
- Purpose limitation – information is shared only for clear, specified and legitimate purposes
- Data minimisation – information shared is adequate, relevant and limited to what is necessary for the purpose of safeguarding pupils
- Accuracy – information is reviewed and kept up to date
- Storage limitation – information is not kept for longer than is necessary for the intended purpose
- Integrity and confidentiality – appropriate security is ensured
- Accountability – compliance with principles is demonstrated

Academies must ensure that information sharing is appropriate for the chosen lawful basis and the applied circumstances. At least one lawful basis needs to be identified prior to sharing

information and academies should ensure that it can demonstrate that it has considered which lawful basis to use in order to satisfy the accountability principle. Records of decisions and reasons for these decisions will be maintained.

The following lawful bases for sharing information will be clearly communicated to staff members:

- Public task
- Legitimate interests
- Legal obligation
- Vital interests
- Consent
- Contract

When sharing special category data – which is sensitive data that includes information about health, or revealing racial or ethnic origin – in addition to identifying a lawful basis the school will ensure that the following is met:

- A condition for processing under Article 9 of the UK GDPR, including health and social care
- For some of those provisions, a condition in the Data Protection Act 2018, including substantial public interest conditions such as the safeguarding of children and individuals at risk

The UK GDPR gives individuals specific rights over their personal data. For general data processing under the UK GDPR, in summary these are:

- The right to access personal data held about them (the right of subject access);
- The right to be informed about how and why their data is used - and you must give them privacy information;
- The rights to have their data rectified, erased or restricted;
- The right to object;
- The right to portability of their data; and
- The right not to be subject to a decision based solely on automated processing.

There are exemptions and restrictions that can, in some circumstances, be legitimately applied to exempt or qualify the right of individuals to exercise their rights. Through sharing information relating to individuals, the above rights remain to apply in certain circumstances and must be processed accordingly (in line with the Data Protection Policy).

7. Data Protection Impact Assessments

Academies must consider completing a Data Protection Impact Assessment for their data sharing activities, to assess the risks to individuals and implement suitable control measures. It may also be necessary to implement a data sharing agreement, considering the below points:

- What is the sharing meant to achieve?
- What information will you share?
- Have you assessed the potential benefits and risks to individuals and/or society of sharing or not sharing?

- Is any of the information special category data (or does it involve sensitive processing under Part 3 of the DPA 2018)? What additional safeguards will you have in place?
- Is it fair to share data in this way?
- Is the sharing necessary and proportionate to the issue you are addressing?
- What is the minimum data you can share to achieve the aim?
- Could the objective be achieved without sharing personal data, or by sharing less personal data?
- What safeguards can you put in place to minimise the risks or potential adverse effects of the sharing?
- Is there an applicable exemption in the DPA 2018?
- How should you share the information? You must share information securely and ensure you are giving the information to the right recipient.
- What is to happen to the data at every stage?
- Who in each organisation can access the shared data? Ensure it is restricted to authorised personnel in each organisation.
- What organisation(s) will be involved? You all need to be clear about your respective roles.
- How will you comply with your transparency obligations? Consider what you need to tell people about sharing their data and how you will communicate that information in a way that is concise, transparent, easily accessible and uses clear and plain language. Consider whether you have obtained the personal data from a source other than the individual and decide what arrangements need to be in place to comply with individuals' information rights.
- What quality checks are appropriate to ensure the shared data is accurate and up to date?
- What technical and organisational measures are appropriate to ensure the security of the data?
- What common retention periods for data do you all agree to?
- What processes do you need to ensure secure deletion takes place?
- When should regularly scheduled reviews of the data sharing arrangement take place?

8. Safeguarding

The UK GDPR does not prevent, or limit, the sharing of information for the purposes of keeping children safe. Lawful and secure information sharing between schools, Children's Social Care, and other local agencies, is essential for keeping children safe and ensuring they get the support they need.

Article 6 of the UK GDPR defines six lawful bases for processing (including sharing) personal information. Where information is shared for safeguarding purposes, there is an expectation on the part of the child or family that the common law duty of confidentiality applies, practitioners will need to consider the lawful basis for setting this aside, prior to making the decision about sharing information. In academies, the bases of "public task" or "legal obligation" are likely to be the most appropriate lawful basis to use when sharing information to safeguard or protect the welfare of a child (e.g. when exercising statutory duties in relation to children under the Children Acts of 1989 and 2004 and other related legislation).

The government Information Sharing Advice (May 2024) details that consent should not be seen as the default lawful basis for sharing personal information in a child safeguarding context because it is unlikely to be appropriate in most cases. The UK GDPR sets a high

standard for consent to be used as a lawful basis; it must be specific, freely given, unambiguous, time limited and capable of being withdrawn by the individual at any time.

Using consent as a lawful basis means an individual has given agreement for personal information about themselves, or their child's personal information, to be shared or processed for a purpose where they have a clear choice about its use. It also means that the individual is able to withdraw their consent at any time. These conditions are unlikely to be present in situations where practitioners are often under a professional duty to record information – irrespective of the wishes of the child or their family – in order to justify the decisions and actions they take in relation to the child's needs, and where the overarching consideration will be whether information needs to be shared to safeguard a child where there is an established or potential risk of harm. Additionally, in some circumstances, seeking consent from a person you believe is neglecting or abusing a child is likely to undermine safeguarding procedures and may increase the risk of harm to the child or another person.

Whenever it is safe and practical to do so, professionals should engage with the child and their family and explain who you intend to share information with, what information they will be sharing and why.

Where seeking to discuss a potential concern would put the child or others at risk of harm, this information should not be shared. Where the child or parent / carer does not have a choice about information sharing, they should still be informed about what information sharing has taken place and how the information will be used, wherever possible and safe to do so.

Informing the child or their parent or carer about the decision to share information must not take place if doing so could put a child or others at further risk of harm, or could compromise effective safeguarding arrangements, including police investigations. In any situation where children or their parent(s) or carer(s) object to particular information sharing, but a practitioner decides that it is appropriate to share the safeguarding information, it is important for practitioners to record their reasons and the legal basis for doing so.

All those who process data should be confident of the processing conditions which allow them to store, and share, the information that they need to carry out their role. Where those staff members need to share special category personal data, they should be aware that the Data Protection Act 2018 includes 'safeguarding of children and individuals at risk' as a condition that allows practitioners to share information without consent in certain circumstances. Information can be shared legally without consent, if a practitioner is unable to, cannot be reasonably expected to gain consent from the individual, or if to gain consent could place a child at risk (DPA 2018, Part 2,18; Schedule 8, 4).

When practitioners in academies are considering whether or not to share safeguarding information (especially with other agencies), they should record who they are sharing that information with and for what reason. If they have taken a decision not to seek consent from the data subject and/or parent/carer that should also be recorded within the safeguarding file. All relevant information can be shared without consent if gaining consent would place a child at risk. Fears about sharing information must not be allowed to stand in the way of promoting the welfare and protecting the safety of children. As with all data sharing, appropriate organisational and technical safeguards should still be in place.

The sharing of personal information must be necessary, fair and proportionate, staff should only share the personal information that is adequate, relevant and limited to what is necessary to protect a child from harm. Requests to share information should explain clearly

what is required and why, clarifying any meaning or terminology where needed to avoid misinterpretation or misunderstanding. If practitioners are in doubt about what information is needed, they must always seek clarification from the requesting agency or organisation. Where staff have concerns about a child and are unsure if they are at risk of harm, they can contact other practitioners who have contact with the child and sharing limited information with them, to see if they hold additional information which gives cause to believe the child is at risk of harm.

9. Security and Confidentiality

Any member of staff or other person associated with an Academy/Trust that handles or shares data will adhere to the following principles:

- The purpose for sharing data is justified and there is a legal basis for doing so
- Data that personally identifies individuals is not used unless absolutely necessary
- Data is only disclosed on a need-to-know basis
- Guidance is sought from the DPO as appropriate
- All data is shared securely (refer to the Information Security Policy)

If personal data is being communicated verbally, it will not be shared in front of other individuals who are not authorised to access the data. Staff members will not disclose or request the disclosure of sensitive data about themselves or others in areas where there are likely to be unauthorised people present, e.g. the Academy reception.

Disclosure of data via the telephone should be conducted in line with the following procedures:

- Verify the identity of the other party on the phone – the type of verification will differ by service and the sensitivity of the data being disclosed
- Establish the reason for requesting the data and ensure this is appropriate
- Request the other party's contact details and check their identity by calling the person via their organisation's main switchboard and asking for them by name
- Only provide the data to the person who requested it (where authorised to do so)
- Do not disclose any personal data via voicemail – be aware that confirming you are a member of an Academy could be considered as releasing personal information
- Take precautions to ensure that data is not shared inappropriately with others, e.g. be cautious if disclosing data on the phone when in a public place
- Do not disclose personal data via text messaging

Disclosure of data via email will be conducted in line with the following procedures:

- Sensitive and confidential personal data will be encrypted and password protected if sent via email
- Passwords shall not be sent to the recipient via email and shall be communicated securely by other means e.g. phone
- Test emails will be sent before sending sensitive, confidential (or bulk) data
- Care will be taken when addressing emails to ensure a correct, current address is used and the email is only sent to those who are authorised to receive the communication and where there is a specific purpose for the information to be shared

- If data is not received by the intended recipient, the contact details and email addresses will be checked to ensure they are correct before resending, the original email is retracted
- Consider what impact any data being lost or misdirected may have – where data is being provided in bulk or is of a sensitive nature, an assessment will be made on the type of protection to be applied
- When transferring data, be aware of who has permission to view your emails or who might be able to view your recipient's emails

Paper-based data will be managed as follows:

- Clear-desk policies are implemented and staff members will ensure that their desks are clear of documents containing personal data at the end of each day or where the information is not attended.
- All files containing personal data will be stored in locked filing cabinets, cupboards or drawers, keys will be held by designated authorised staff only.
- Sensitive data will be held securely at all times, i.e. stored in a locked filing cabinet, cupboard or drawer and in a locked bag if the data is being transported.
- Data which requires sharing in paper format will be hand delivered where possible or sent via recorded post.

If 'middleware'/'data integrators' that extract data from the MIS are to be used in other systems are in place, for example, Groupcall Xporter, Wonde, OvernetData, SalamanderSoft, Assembly/Ark UK group and Ruler, it is vitally important that Academies are aware of what information is being extracted from their MIS and how it is being used and/or shared with other systems, and that this sharing is compliant. A DPIA should be completed to assess the risks accordingly.

The Information Security Policy is referred and adhered to when managing the security of personal and confidential information.

Appendix One

Data Sharing Decision Form Template

Name of organisation receiving request to share data	
Name of organisation requesting data	
Name and position of person requesting data	
Date request received	
Description of data requested	
Data controller relationship	☐ Joint ☐ Separate
Will we have a data sharing agreement in place?	☐ Yes ☐ No
Purpose of sharing	
Lawful basis for sharing	
Why is sharing 'necessary'?	

Are additional conditions met for special category data or criminal offence data sharing (where applicable)?	
Have you considered a DPIA?	
DPIA undertaken and outcome (if applicable)	
Were views of DPO (or equivalent) considered? (if DPIA not done)	
Are there any specific arrangements for retention/deletion of data?	
What are the security considerations?	
What arrangements are there for complying with individuals' information rights?	
Date(s) of requested sharing (or intervals if data is to be shared on a regular basis)	
Decision on request	
Reason(s) for sharing or not sharing	
Decision taken by (name and position)	
Signed	
Dated	

Appendix Two

ICO's 10 Step Guide to Sharing Information to Safeguard Children:

https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-sharing/a-10-step-guide-to-sharing-information-to-safeguard-children/

Appendix Three

DfE non statutory information sharing advice for practitioners providing safeguarding services for children, young people, parents and carers

Appendix Four

The Working Together on Safeguarding Children statutory guidance states the following:

1. Effective sharing of information is essential for early identification of need, assessment, and service provision to keep children safe.

2. All professionals responsible for children should be proactive in sharing information as early as possible to help identify, assess and respond to risks or concerns about the safety and welfare of children, whether this is when problems are first emerging, or where a child is already known to local authority children's social care (e.g. they are being supported as a child in need or have a child protection plan). You should be alert to sharing important information about any adults with whom that child has contact, which may affect the child's safety or welfare.

3. Information sharing is also essential for the identification of patterns of behaviour when a child has gone missing, when multiple children appear associated to the same context or locations of risk, or in relation to children in the secure estate where there may be multiple local authorities involved in a child's care.

4. Fears about sharing information must not be allowed to stand in the way of the need to promote the welfare, and protect the safety, of children, which must always be the paramount concern. To ensure effective safeguarding arrangements.

Information should be shared in a timely fashion to reduce the risk of missed opportunities to offer support and protection to a child. Timeliness is key in emergency situations, and it may not be appropriate to seek consent for information sharing if it could cause delays and therefore place a child or young person at increased risk of harm. Practitioners should ensure that sufficient information is shared, as well as consider the urgency with which to share it.