Staffordshire University Academies Trust		Trust Policy Document			
Approved by:	**Trust Board**	**Issue date:**	**Sept 2023**	**Review date:**	**Sept 2024**
Policy Owner:	**DPO**	Page: **1 of 12**			
Audience:	**Trustees** ☑ **Staff** ☑ **Pupils** ☑ **Local Academy Council** ☑ **Parents** ☑ **General Public** ☒				

Data Sharing Policy

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.

Policy Aims

This policy aims to:

- Assure individuals whose data the Academies and Trust process;
- Provide greater 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 risk when sharing data;
- Provide more robust sharing practices and better protection for individuals whose data is shared;
- Demonstrate compliance with the law.

Data Sharing Definitions

There is no formal definition of data sharing within data protection legislation, although the scope 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.

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.

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.
- 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, family members, friends or other associates 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, downloading 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 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.
- Ensure 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 and that procedures for identifying, reporting and managing any breach are in a timely manner, by following the data breach management plan.
- 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.
- Staff are appropriately trained.
- Breaches in relation to the sharing of data are appropriately reported.
- That data is redacted or anonymised where necessary.

Information Sharing Guidance

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

- Remember that the UK General Data Protection Regulation (GDPR), Data Protection Act 2018 and human rights law are not barriers to justified information sharing but provide a framework to ensure that personal information about living individuals is shared appropriately.
- Be open and honest with the individual (and/or their family where appropriate) from the outset about why, what, how and with whom information will, or could be shared, and seek their agreement, unless it is unsafe or inappropriate to do so.
- Seek advice from other practitioners, or your information governance lead, if you are in any doubt about sharing the information concerned, without disclosing the identity of the individual where possible.
- Where possible, share information with consent, and respect the wishes of those who do not consent to having their information shared. Under the UK GDPR and Data Protection Act 2018 you may share information without consent if there is a lawful basis to do so, such as where safety may be at risk. You will need to base your judgement on the facts of the case. When you are sharing or requesting personal information from someone, be clear of the basis upon which you are doing so. Where you do not have consent, be mindful that an individual might not expect information to be shared.
- Consider safety and well-being: base your information sharing decisions on considerations of the safety and well-being of the individual and others who may be affected by their actions.
- Necessary, proportionate, relevant, adequate, accurate, timely and secure: ensure that the information you share is necessary for the purpose for which you are sharing it, is shared only with those individuals who need to have it, is accurate and up to-date, is shared in a timely fashion, and is shared securely (please see principles within the Data Protection Policy).
- Keep a record of your decision and the reasons for it – whether it is to share information or not. If you decide to share, then record what you have shared, with whom and for what purpose.

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 always 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.

When
Is there a clear and legitimate purpose for sharing information?
• Yes – see next question
• No – do not share

Do you have consent to share?
• Yes – you can share but should consider how
• No – see next question

Does the information enable an individual to be identified?
• Yes – see next question
• No – you can share but should consider how

Have you identified a lawful reason to share information without consent?
• Yes – you can share but should consider how
• No – do not share

How
• Identify how much information to share
• Distinguish fact from opinion
• Ensure that you are giving the right information to the right individual
• Ensure that you are sharing the information securely
• Where possible, be transparent with the individual, informing them that that the information has been shared, as long as doing so does not create or increase the risk of harm to the individual or there is a legal reason not to. All information sharing decisions and reasons must be recorded in line with Academy procedures. If at any stage staff are unsure about how or when to share information, they should seek advice on this.

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. 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.

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 that was recorded
- The lawful basis for processing and any additional conditions applicable
- Individuals' rights
- Data protection impact assessment reports
- 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 should be accompanied by a DPIA and will depend on the nature, scope, context and purposes of the sharing.

Data Protection Impact Assessments

Academies may 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 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?
- 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. 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.

- 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?

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. 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. 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 Designated Safeguarding Leads in Academies are considering whether, or not, to share safeguarding information (especially with other agencies) it is considered best practice for them to 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 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.

Security and Confidentiality

Any member of staff or other person associated with the 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 in person, 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 sensitive personal data via text messaging

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

- Sensitive personal data (or bulk records) will be encrypted if sent via email
- Test emails will be sent before sending sensitive (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 with a legitimate interest and who are authorised to receive the communication
- 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:

- The Academy implements a clear-desk policy wherever possible and staff members will ensure that their desks are clear of documents containing personal data at the end of each day
- All files containing personal data will be stored in locked filing cabinets, cupboards or drawers
- 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

If 'middleware'/'data integrators' that extract data from your MIS 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.

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

Data Storage, Sharing and Security – FAQs from the Information Commissioner's Office; the link is provided as follows - https://ico.org.uk/for-organisations/sme-web-hub/frequently-asked-questions/data-storage-sharing-and-security/