DfE Data Protection Strategy:

Looking at the role of data integrators and more specifically the following:

The types of questions schools should be asking

- Is the data integration necessary for the purpose?
- Could the purpose be fulfilled safely without data integration?
- Will data integration improve the service being provided?
- Will data integration increase/reduce any risks related to use of the personal data?
- Is the data integrator compliant with current data protection laws, including but not limited to DPA2018 and GDPR?
- How can they demonstrate their compliance?
    - Accreditations?
    - GDPR compliant contracts?
    - Compliance statement / assurances
    - Case studies/references?
    - Codes of Conduct?
- Are they accredited to any information security or data protection standards?
    - ISO 27001
    - Cyber Essentials
    - Government G-Cloud Framework
    - ISO 9001
    - PCI DSS
    - Has the service been independently penetration tested by a CREST approved external supplier?
- Is there a clearly defined Data Sharing Agreement setting out:
    - What types of personal data the data integrator will process
    - What categories of data subject the personal data relates to
    - What purpose this data will be used for
    - How long it will be processed/retained
- Does the contract with the data integrator include terms/clauses stating that they will:
    - Process the personal data only on your instructions
    - Ensure any staff processing the data are subject to a duty of confidentiality
    - Take appropriate measures to ensure the security of the processing
    - Only engage a sub-processor with your prior authorisation and under a written contract
    - Take appropriate measures to help you respond to requests from individuals to exercise their rights
    - Assist you in meeting your GDPR obligations
    - Delete or return all the personal data to you (at your choice) at the end of the contract and delete existing personal data unless otherwise required by law
    - Submit to audits and inspections as well as providing you with whatever information you need to ensure you are both meeting your Article 28 obligations

- Will the data integrator be processing only as much personal data as is required for the purpose or are they going to be processing more than is required for the purpose?
- Will you have control over the personal data they are able to access/process?
- Will you have control over the data subjects whose data the integrator will have access to?
- Wil you be able to add data subjects and remove data subjects as necessary?
- Will you have control over which third-party organisations the data integrator provides the personal data to?
- Will you be able to switch off the data flow to one or all third-party organisations as you deem necessary (for instance where you suspect a data breach caused by one of the organisations etc.)?
- Will you have complete visibility of all organisations to whom the data integrator is providing the personal data?
- Will you have complete visibility of all personal data that the data integrator is providing to each third-party organisation through specification of the data scopes being provided and the data subjects included in each integration?
- Will you have complete visibility of where each third-party hosts your data?
- Are you able to easily obtain all the information necessary to comply with a Subject Access Request if you were to receive one?
- Are you able to easily arrange the deletion of personal data, either directly yourselves or via the data integrator, should it be necessary?
- Do you have full visibility of the automated data lifecycle, for example how long off-roll students are retained in the data?

The typical scenarios that schools can control

- ***Which data integrator you allow to have access to your data***.

  Some third-party organisations may try to insist on a specific data integrator because this is who they have a relationship with but, as data controller, the final decision on use of processors is yours and it is your responsibility to be confident that all processors, including the data integrator, is compliant etc. The third-party organisation may have commercial reasons for wanting to use a specific integrator and so it is important to ensure that the integrator used meets your security and safety as well as the requirements of the third-party organisation.

- ***Which third-party organisations you allow the data integrator to provide your data to***.

  No one is allowed to process your data other than on your instructions and this includes the data integrator. The fact that you have allowed the data integrator to process your data to provide it to one third-party organisation does not give them permission to provide it to another third-party organisation without your consent. Ensure you have control of this.

- ***What personal data you allow each third-party organisation to be provided with by the data integrator.***

This should be clearly specified in the data sharing agreement between your school/Trust and the third-party organisation but also look for the ability within the data integrator's management module for you to be able to see what personal data is being provided and the ability to enable or disable the various personal data items yourself.

- ***Which data subjects or groups of data subjects' personal data is processed by the data integrator.***

  Look for the data integrator to provide you with the ability to allow or disallow personal data on specific pupils/staff/parents to be processed. You may need to have the personal data of some pupils to be processed – for instance, those with safeguarding issues – but not all pupils. The data integrator should provide you with tools to manage this so that you control whose data is processed and can change this at any time

- ***Which data subjects or groups of data subjects' personal data is provided by the data integrator to specific third-party organisations.***

  Again, look for the data integrator to provide you with the ability to allow or disallow personal data on specific pupils/staff/parents to be provided to each third-party organisation you authorise. You may need to have the personal data of some pupils to be provided – for instance, those with safeguarding issues – into a third-party safeguarding platform, but not all pupils. The data integrator should provide you with tools to manage this so that you control whose data is provided to which third-party organisation and be able to change this at any time

The typical scenarios that schools can't control

- ***The core personal data required by each third-party organisation***

  Each third-party organisation that you authorise to process personal data on your behalf will have a set of required data items that it needs in order to provide the service to you. Without receiving these data items, the third-party will not be able to provide the service to you and so you have no choice, if you wish to use their service, other than to allow them to have these required fields. However, you should assess the data items they say are required to ensure you agree that these are necessary. An example would be parental contact details. Does the third-party need to contact the parents or send them information? If not, then why do they need these items?

- ***The frequency at which the data is updated by the data integrator***

  The data integrator will schedule the processing of the personal data from your MIS and the frequency at which this occurs will usually be driven by the data integrator who will be attempting to keep the data within the third-party organisations as up-to-date and accurate as is reasonable. There will usually be a core processing overnight for those data items that do not change frequently or do not need updating regularly together with a more frequent

processing of data that does change regularly such as attendance information which changes according to when attendance is updated in your school.

- ***The frequency at which the data integrator provides the data to the third-party organisations***

  The third-party organisation will require the personal data to be kept up-to-date and accurate as far as is reasonable to ensure that they provide you with an effective service. Some will need the data updated regularly throughout the working day (such as attendance systems, behaviour software, safeguarding software etc) whilst others will only need the data updated infrequently.

- ***Breaches of confidentiality by the data integrator's staff***

  Whilst you are unable to control this, nor prevent it, you can take steps to mitigate the impact of this on your school/organisation by ensuring that you have the correct contracts in place with the data integrator. These contracts should include a clause to the effect that the data integrator will ensure all its staff involved in processing your data will observe confidentiality of this data. You should also ask them for information on the training provided to their staff around data protection in general and the GDPR specifically – the better this training, the less likely a breach of confidentiality since their staff will better understand their data protection responsibilities. Remember, it is not a requirement for every member of the data integrator's staff to have a Disclosure Check, so don't demand that all are subject to this. Any of their staff that visit schools are required to have a Disclosure Check and you can certainly ask for confirmation of this.,

- ***Data breaches caused by the data integrator software or processing***

  Again, whilst you are unable to prevent data breaches happening which are caused by the data integrator or its software, you can mitigate this and make them less likely to occur by ensuring you do your due diligence before agreeing to the use of the data integrator. Ensure you ask the questions outlined above, make sure a compliant contract is in place and get some information about the training provided o the data integrator's staff.

- ***Data breaches caused by third-party providers who get authorised personal data from the integrator***

  As with breaches caused by the data integrator or its software, you cannot prevent such breaches happening as a result of a failure or error on the part of the third-party organisations who are processing your data in order to provide their services to your school/organisation. However, once again, you can mitigate against this by undertaking appropriate due diligence of the third-party before allowing them access to the data, making sure you have appropriate compliant contracts in place etc.

Some real life "what really can happen"

- ***School staff authorise more personal data to be processed than is necessary***

School staff are busy people and it can be easy to simply authorise the data integration without checking everything is as it should be. Remember to check that the personal data being asked for is genuinely required for the purpose for which the third-party organisation processes it.

- ***Data integrator processes more personal data than is required for the purpose***

  Data integrators will require high-level access to school data in order to be able to extract the required data and provide it to the third-party organisations approved by the school. Check that they are only extracting the data that is actually required to provision all the approved third-party organisations needs. Some integrators may extract all available data without needing it all, on the basis that they are ready for whenever another approved third-party requires it. This would not be necessary so check that they are only extracting what is actually needed to provision those approved currently. If further data is required by a newly approved third-party, the integrator should be able to extract that at that point and not before.

- ***Data integrator passes personal data to a third-party which has not been approved by the school***

  Your data integrator will have contracts with many third-party organisations to provide them with the personal data they need to provide services to schools. It is important to ensure that the data integrator provides you with the ability to control who your data is passed to. It should not be possible for the data integrator to pass data to a third-party that has not been explicitly approved by yourselves.

- ***Data integrator passes personal data to the wrong third-party provider***

  The data integrator will be providing integration services for many third-party organisations. Ensure that there are clear identifiers for each third-party and extensive safeguards that are designed to prevent data being passed to the wrong organisation. The integrator should have controls that make it extremely difficult for mistakes to be made, including passwords, usernames and/or two-factor authentication etc. as well as clear and actionable approval processes that you control.

- ***School level data is passed to the correct third-party but for the wrong school***

  All data integrators will be providing integration services for many schools and so there is a danger that they extract data from one school and provision it to a third-party organisation as coming from another school. The integrator should have in place separation of data between schools, protection via passwords, usernames and/or two-factor authentication to ensure this does not occur. In addition, ask if they have cross-checks in place that would immediately alert them to any potential disconnect between the originating school's data and the expected recipient school's data within the third-party organisation.

- ***School staff email unprotected personal data to the data integrator***

There should be no reason at all for your staff to have to send personal data to the integrator by email, or indeed any other method. The whole purpose of the data integrator is to remove such means of data transfer by automating it and making it far more secure. Whilst the integrator will almost certainly insist that no data is passed to them by these means, it still happens regularly, causing potential data breaches and additional work for all concerned in deleting the unwarranted spreadsheets of data etc. Make sure all your staff are trained and know that they should never be sending personal data in this way

- ***Incorrect personal data against an individual is processed***

  This can occur but is usually the result of inaccuracies within your Management Information System, caused frequently by human error such as typing errors, copy and paste errors etc. All your pupils, staff etc. will have unique identifiers within your MIS which will be used to ensure no mistakes like this occur, but if your staff have entered duplicated UPNs etc. then a data breach could occur. Emphasise the need for accuracy and checking whenever your staff are entering or editing personal data to ensure the likelihood of this type of breach is minimised.

- ***MIS updates cause integration to fail***

  Your school MIS will initiate upgrades and updates regularly and these frequently alter the configuration which in turn causes the integration to fail due to this mis-configuration. Ensure that when you are informed of any MIS updates etc. you let your data processors and/or data integrator know about these

- ***School level issues cause integration to fail***

  Passwords that provide the required access for the data integrator frequently get changed by IT staff as part of regular password change policies etc. If these access passwords are going to be changed you must ensure that you let the data integrator know the new passwords to make sure the various data integrations continue. Failing to do so will cause all the third-party solutions that rely on the data integrator to fail.

- ***School infrastructure changes cause integration to fail***

  Changes to your infrastructure, be that new servers being installed, new software etc. can cause the integration to fail because the configuration has changed. Always ensure that your IT staff speak with the data integrator in advance of such changes so that a process can be agreed to ensure continuity of the various services reliant upon the data integration.

- ***Simple, school level errors/accidents cause the integration to fail***

  These errors can be as simple as an accidental switching off of a server by untrained staff or cleaning staff unplugging it or accidentally knocking the power switch into the off position. If you notice that the integration has failed, always check for these accidental impacts.

List risks associated with the above that are not to do with systems but process

- Inaccurate recording of personal data within the school MIS leading to inaccuracies in third-party systems being used by the school
- Failing to keep the personal data up to date in the MIS leading to inaccuracies in third-party systems being used by the school
- Staff member approving third-party processing without authority
- Staff member approving third-party processing without checking the data is sufficient for the purpose and no more
- Staff member approving third-party processing for more data subjects than necessary
- Staff raise support case by email and include personal data in the email in order to 'evidence' the issue
- School failing to undertake due diligence of third-party processors
- School failing to have compliant contracts and DSA with third-party processors
- DPIA not being undertaken when required