**Data Protection and Remote Learning**

As you will be aware, the Secretary of State for Education recently issued a direction for schools to ensure they have a contingency plan for the continuity of education in the event pupils cannot attend schools as a result of COVID-19.

Data protection will probably not be your number one concern right now, but it is important to ensure you are considering your data protection obligations in any plans for remote working and the delivery of education via alternative means.

The DfE have provided some guidance on good practice for remote learning, which can be found by clicking [HERE](https://www.gov.uk/government/publications/remote-education-good-practice/remote-education-good-practice).

If you are introducing a new system, or processing data in a new way, we have outlined below some points you will need to consider to ensure you are fulfilling your data protection obligations:

* **Your lawful basis for processing**: processing that is directly linked to the provision of education can be justified as under your duty to fulfil a public task. Therefore, from a GDPR perspective, you will not need to obtain consent from parents or students before processing their data for the purposes of remote education. However, if you are required to share any special category data, you will need a second justification for this. If this is the case, please contact your DPO to discuss why you will need to share the data.
* **Conduct a Data Protection Impact Assessment**: The overall aim of a DPIA is to capture the detail of the processing and to ensure you have identified the risks to individuals’ rights and freedoms and identified steps to mitigate those risks.

*If you are subscribed to Warwickshire Legal Services’ School DPO Service, please look out for our next bulletin which will include an exemplar DPIA.*

* **Ensure you have the relevant assurances in place as required by Article 28 of the GDPR**: Essentially, you need to identify where any third parties that you use store their data – if this is outside of the UK or European Economic Area, additional checks will need to be made. If they are within the UK or the EEA, you need to be sure that any contract or agreement with the third party includes the adequate data protection clauses. *The DPO Service will happily review any third-party agreements on behalf of our subscribing schools.*
* **Update your privacy notices**: you should add details of what data you are processing and who you are sharing the data with, to the relevant privacy notices (I.e., Privacy Notices for staff and pupils). You would need to be proactive in bringing this update to the attention of individuals. Most schools will specifically write to pupils and parents to advise them of their plans for delivering education remotely. You may wish to include information on this update and refer individuals to the privacy notice at this point. If you are not specifically writing out to parents, then consider how else you can achieve this? E.g., including information within your school newsletter.
* **Information Security:** Ensure you liaise with your IT support to ensure you are using a secure platform and that the transfer of any data is done so in a secure manner.
* **Keeping children safe online:** This is where your safeguarding obligations meets your data protection obligations. As well as data protection requirements, there may be certain requirements placed on the school for safeguarding purposes, so it is vital that you consult with your safeguarding lead on any online systems you will be asking children to engage with. You will also need to consider the types of data you will need to share in order to fulfil the purposes of remote education. You should only share the data that is considered necessary to allow you to achieve the required purpose. We also take this opportunity to remind you to you consider any privacy settings of any online platforms you are planning to use.

Although you are probably not seeking consent for the processing/sharing of data in this way, it is important to remember that individuals have the right to object to the processing. More detail about this will be included in the next data protection bulletin. Should you receive an objection, we would recommend that you contact your DPO for advice.

**Staff working remotely**

Consider how staff will access personal information when working from home. Ideally staff should be able to access the school’s network in a secure way. You should discuss this with your IT support to identify the most secure way for staff to continue to work effectively from home.

Some secure methods would include:

* Accessing a secure cloud-based system
* Using a VPN connection
* Utilising the use of Multi factor authentication
* Ensuring staff have access to use a secure (encrypted) device.

Remind staff of your school’s Information Security Policy to ensure they are implementing this in their home. E.g. ensuring any paper documents are kept secure and disposed of in a secure manner. Keeping their computer screens locked when unattended, the importance of using secure methods of communication (such as using their school email address for communications).

We appreciate that this is a lot of information to take in and it can possibly feel a little overwhelming. However, rest assured that the School DPO Service are on hand to assist all our subscribing schools in any way we possibly can.