COVID-19 & Data Protection

Newsletter

Date/Version : 16 March 2020

The aim of this newsletter is to raise awareness for the potential Data Protection issues caused by COVID-19 and how schools might mitigate them.

Data sharing with public bodies

Schools may be required to share information with public bodies regarding pupils and staff who have contracted the virus. This would be a valid processing activity but would need to be supported by your internal processes and documentation.

The fact that you will share data with public bodies should be present in your:

- Record of Processing Activity
- Privacy Notices

Accompanied by the fact the school use the following lawful bases to do so:

- Article 6(1)(e): Carrying out a specific task in the public interest (personal information)
- Article 9(1)(i) Public health (with a basis in law) (Medical)

Information sharing with parents and staff

Careful consideration should be given regarding how, when and if any communications should be made to inform the school population about the medical status of a pupil or member of staff.

First always consult the current Public Health England guidance:
https://www.gov.uk/government/collections/coronavirus-covid-19-list-of-guidance

It is our Data Protection advice that unless directed otherwise by Public Health England, you should avoid mass communications regarding if an individual is self-isolating where there is no confirmed COVID-19 diagnosis.

Communications between need to know individuals as part of an absence or sickness reporting protocols is fine and covered under your current documentation and protocols.

If the school feels that the absence of staff and pupils needs to be addressed, then a generic statement could be given:

‘ *you may notice that some staff and some pupils are absent from school. This is because we are all following government advice and staying away from school for 7 days if any staff member or pupil has a cough or temperature. This doesn’t mean they have COVID-19; it simply means that we are following government guidance*

to ensure the school community is as safe as possible in the current situation'

If there is a confirmed diagnosis and a communication is required, then singling out an individual should be avoided, and generic information used instead:

i.e. Jo Smith has COVID-19 vs a pupil in year 5 Poplar class has COVID-19

Staff should be reminded that any communications should come through official channels only and discussing confidential information about people's medical health is a data breach and will be treated as such.

Skeleton crew

Even if it was inappropriate for all school staff and children to attend the school, a small "key" band of personnel could still work from the school site if the risk of their data processing is be deemed to be too high.

This might include those who process SEN, Safeguarding, Admissions and Finance where the removal of the data from the school site is impractical.

Remote Working

If you work from home and this is not a usual practice for you, and you are going to be providing staff with the ability to do so, there are a number of considerations:

ICT User Agreements:

- Have they been updated to reflect that individuals will be working remotely, or do you need to make a one-off ICT user Agreement for this scenario?
- It is important that people know exactly what the school expects from them in order to comply.

Personal devices vs school devices:

- Are you able to provide school devices for individuals to work from home, or will they need to use their own personal devices?

Personal devices carry a greater risk as they can be shared within a household. This means the following should be considered:

- Temporary internet files being retained (can be viewed by others using the device)
- Saving to desktop (can be viewed by others using the device)
- Autosaving log in passwords (allows others to access)

In addition, the personal device may not be as secure as a work device due to:

- Lack of encryption
- Lack of antivirus
- Lack of system updates or using outmoded software

Paper documentation:

Most residences do not have the same level of available lockable storage facilities as a school. Therefore, what paper documentation, if any, should be taken home to work remotely should be considered.

If items are not securely locked away, they can be accessed by other people in the house or simply lost. DPO recommendation is that no special category data or confidential material should be taken from the school site nor should lists containing more than 2 pieces of personally identifiable data.

Staff who do take paper documentation home with them should be reminded of the necessity of keeping data as secure as possible.

Electronic data transfer:

If staff are going to be working remotely or preparing to work remotely, they may need to transfer data from the school site to home. This would still need to be done in a secure manner:

- If Flash drives/USB sticks/memory sticks are going to be used, and data is going to be present, they must be encrypted. It is too easy to lose these items and have a breach.
- Additionally, the school and the teacher/staff member should make a note that this is occurring, so a reminder can be sent afterwards to delete the data when it is no longer needed.
- If individuals will be emailing resources to a different account to access it from home, then again, if this is a shared account, data should not be present (like governors for example). In addition, as with USB devices, it should be noted so that it is deleted when it is no longer needed.

Grow Education Partners supports over 200 schools in meeting their statutory Data Protection duties with ongoing guidance and advice. To discuss any item in this newsletter, please contact david.coy@london.anglican.org. Alternatively, you can find out more about our Data Protection services here ›