IGS COVID 19/Data Protection FAQ and Tips for schools

As schools move toward temporary closure we have put together some commonly asked questions and answers to assist schools in remaining compliant with Data Protection obligations. Changes to working practices can often create additional risks or personal data breaches, but we are here to support you.

Please note that for our customers our helpdesk will remain open throughout this crisis to give advice and support. If your school is not a current customer and you would like to sign up to receive a service and support, please get in touch by contacting IGS@essex.gov.uk or calling 03330 322970.

Q. Can we give students access to laptops and the network?

A. It is fine to provide the students with laptops and network access if the laptops are locked down to ensure they can only access student areas. Make sure the student is given their own login rather than a staff member sharing their password. Ensure your web filters are set to block malicious or explicit content.

Q. We have been approached by Tesco to share parents' email addresses to allow Tesco to send email vouchers to the parents of the recipients of free school meals, what do we need to do to share these emails?

A. Whilst it is a worthwhile cause, most parents would not expect their email address to be shared with a third party. It is also likely that the recipient would think that the email is SPAM if they are unaware that it is coming. Speak to the parents and inform them of this provision and seek their consent to share their email address with Tesco.

Q. Can staff access the IGS eLearning if working from home?

A. Yes! The course can be accessed from home. Please let us know if you need any help logging on or if any new members of staff would like to access the course.

Q. Can staff take papers to work on from home?

A. It would be preferable to take the information home on an encrypted memory stick. However, if paper is necessary then please follow the tips below.

Q. If working at home should we share information with other Professionals, e.g. social or health workers if asked?

A. You should have a process in place to verify the requestor is legitimate. This may become more difficult as Professionals are required to work from home and their calls may not be routed through call centres. You must still find a way to satisfy yourself that they are who they say they are by asking questions which they should know the answer to, or by calling the organisations switchboard (confirmed online) to verify the caller's name and

position. If in doubt, **unless it places a child at risk of harm**, you should not share personal data.

Tips

1. Make sure any laptops/papers/memory sticks are kept with staff in transit and out of sight at their homes. School information should be kept secure overnight, preferably locked away.
2. If you need to communicate with all parents by email, make sure you blind copy all parents email addresses by using the bcc function.
3. Make sure staff do not email documents (containing personal information) to their personal email addresses.
4. Any laptops/memory sticks/hard drives leaving the school should be encrypted.
5. Any records leaving the school site should be tracked to ensure it is clear whose possession they are in and where they are so that they remain accessible to other staff; and also to record when they were returned to the school site.

If you require our support with any data protection concerns please do get in touch.

Keep safe and well.