GUIDANCE FOR NON-SCHOOL BASED EA STAFF

Data Protection and Coronavirus (COVID-19) Frequently Asked Questions

Can we collect health data in relation to COVID-19 about staff?

You have an obligation to protect the health of your staff, but that doesn't necessarily mean you need to gather lots of information about them. It is however reasonable to ask people to tell you if they are experiencing COVID-19 symptoms. Don't collect more health data than you need and ensure that any information collected is treated with the appropriate safeguards to ensure confidentiality.

Can we share employees' health information with authorities for public health purposes?

Yes. If it is necessary for you to share information with authorities about specific individuals for public health purposes, then data protection law won't stop you from doing so.

During the pandemic, we are worried that our data protection practices might not meet our usual standard or our response to information rights requests will be longer. Will the ICO take regulatory action against us?

No. The ICO has confirmed that it understands that resources, whether they are finances or people, might be diverted away from usual compliance or information governance work and that it won't penalise organisations that it knows need to prioritise other areas or adapt their usual approach during this extraordinary period.

The ICO has also confirmed that whilst it can't extend statutory timescales, it will tell people through its own communications channels that they may experience understandable delays when making information rights requests during the pandemic.

The ICO has also confirmed that it will be taking the same pragmatic approach in relation to any delays in responding to FOI requests during the pandemic.

More of our staff will be homeworking during the pandemic. What kind of security measures should we have in place for homeworking during this period?

Data protection is not a barrier to increased and different types of homeworking. During the pandemic, staff may work from home more frequently than usual.

Data protection law doesn't prevent that, but you'll need to consider the same kinds of security measures for homeworking that you'd use in normal circumstances.

What responsibilities do EA staff have when working remotely?

Any member of staff working remotely is responsible for ensuring that they work securely and protect both personal information and EA-owned ICT equipment from loss, damage or unauthorised access.

What responsibilities do EA staff have when working remotely using ICT equipment?

The EA's Acceptable Use of ICT Policy applies to the use of EA ICT equipment at home in exactly the same way as if you were working in the office and you must therefore adhere to that policy at all times when using EA ICT equipment outside the office.

EA staff should not develop or propose remote solutions outside of those approved by EA's ICT Services. Any ad-hoc solutions pose both a security and capacity risk to the continued operation of services across EA. ICT Services staff will continue to work on the provision of remote working solutions and staff must follow any guidance published by ICT Services in this respect.

Whilst under normal circumstances EA staff would be advised not to use non-EA computers for work purposes, given the situation we are facing, EA's ICT Services have confirmed that staff who do not have an EA laptop can access webmail from their home computer if necessary (preferably using Internet Explorer or Edge browsers) provided that they use this facility with caution. EA's ICT Services have confirmed that it is safe to open emails, reply to them, or create new emails using webmail. Staff must not however download attachments, or attach documents produced on their home computer, unless this is completely unavoidable.

Webmail can be accessed at https://webmail.eani.org.uk

You must not make any modifications to EA ICT equipment unless it is authorised by EA's ICT Services. Also, you must not connect any non-EA ICT equipment to any EA ICT equipment with which you have been provided with to enable you to work remotely.

You must take care when connecting to EA's network or when working on a document offline (i.e. without connecting to EA's network). In particular, you should ensure that you are not in a place where anyone could overlook your screen.

You must not allow non-EA staff members (including family and friends) to use the EA's ICT equipment. If creating an EA work document on or downloading an EA work document to a home computer is completely unavoidable then staff should take steps to ensure that such documents cannot be accessed by non-EA staff members (including family and friends) by password protecting such documents immediately after creation or download and (where possible) by not allowing others to use the home computer whilst such documents are on it. In such circumstances it is also crucial that any such document is permanently deleted from the home computer as soon as it is no longer unavoidable to have it on such computer.

If you have direct access to EA's network, you will have the same access as if you were in the office so there is a significant information security risk if used incorrectly. Steps should be taken to store EA ICT equipment securely at home, locking it away either during the day whilst not working on it and at the end of each working day. This also applies to any home computer with EA work documents on it (i.e. where it is has been completely unavoidable to create an EA work document on or to download an EA work document to a home computer).

If you are working on a computer but move away from your screen for any reason, you should lock it.

Are there likely to be any increased cybersecurity and Coronavirus-related Phishing threats when working remotely using EA ICT equipment?

Staff should remain vigilant of increased cybersecurity threats, some of which may specifically target remote access arrangements. Unfortunately, cybercriminals will not be curtailing their efforts to access valuable data during the pandemic, and in fact, will likely seek to take advantage of some of the confusion and communication issues that might arise under the circumstances.

Staff should also be vigilant of phishing emails with malicious links disguised as EA coronavirus updates or as updated EA policies relating to it. If staff are unsure about any email they receive, they should not open the email or click on links without contacting EA's ICT team for advice first.

Can EA staff take paper files containing personal information out of the office for homeworking and what kind of security measures should we have in place for homeworking with paper files?

The use, transportation or storage of hard copy documents containing personal information is a high information security risk when working remotely.

Therefore, where possible, the use of paper documents containing personal information out of the office should be kept to a minimum.

However, where it is necessary to take paper files out of the office, a log must be kept by the relevant EA service recording when any paper file is taken out of the office. This log must record a file reference and a description of the nature/contents of the file, the EA officer that has taken the file out of the office, the date it was taken out of the office and the date the file is returned. The EA officer that takes the file from the office must sign the log entry when they remove the file from the office and when the file is returned to the office.

Where there is a need to take paper files out of the office, the papers should be securely bound within an appropriate folder – not a loose bundle of papers. Paper files should be carried in an appropriate bag or box so that they are not on display and there is less risk of them being dropped. The officer taking the papers should go straight home with the papers.

Steps should be taken to store papers securely at home, locking them away either during the day whilst not working on them and at the end of each working day.

Any documents which need to be disposed of should not be disposed of whilst working at home. They should be brought back into the office and securely disposed of using EA's established confidential waste disposal process. Such documents should be stored securely until you are able to arrange this. As always, staff must adhere to EA's Interim Combined Legacy Retention and Disposal Schedule which is available on the 'Think Data' intranet page - https://sharepoint.eani.org.uk/resources/thinkdata/Pages/default.aspx or on request from the EA's Information Governance team by calling 028 8241 1300 or emailing infogov@eani.org.uk.

When working from home you should ensure that you are not in a place where anyone could overlook the papers you are working on.

As EA staff will have to rely more on the use Skype, video conferencing and telephone calls, is there any advice which staff should follow in this respect?

Where you are in contact with other EA staff, customers or external stakeholders using Skype, video conferencing or telephone, you should ensure that you cannot be overheard by members of the public, other members of the household or any visitors.

What else should we do to ensure that EA does not breach its data protection obligations during the pandemic?

Whilst the advice issued by the ICO referred to above highlights that it may not be possible for data controllers to meet their usual standards in all respects (e.g. it may not be possible to respond to information requests received within the usual statutory timeframes), EA should adhere to the usual standards of data protection during the COVID-19 pandemic to the extent reasonably possible.

In particular, EA should continue to exercise the usual standard of care when processing personal information relating pupils (and their families) and EA staff.

Any personal information relating to pupils (and their families) or EA staff should continue to be processed and communicated in a way that ensures that there is no unauthorised access to such information.

As always, care should be taken to ensure that the contact details which we hold for pupils (and their families) and EA staff (e.g. home addresses, email addresses and telephone numbers) are accurate and up to date, and that care is taken to ensure that all communications containing personal information are correctly addressed.

What should staff do if a Personal Data Security Incident is confirmed or suspected when working remotely?

All staff must report any loss or suspected loss, or any unauthorised disclosure or suspected unauthorised disclosure, of any EA-owned ICT equipment or personal data immediately to their line manager and the EA's Information Governance Team by emailing a Data Breach Report Form to dpo@eani.org.uk followed up immediately by a phone call to the EA's Information Governance Team on 028 8241 1300 to advise that a Data Breach Report Form has been sent.

If a personal data security incident is suspected or confirmed, staff should follow the EA's Data Breach Management Procedure which includes the data breach report form to be used. This procedure is available on the 'Think Data' intranet page - https://sharepoint.eani.org.uk/resources/thinkdata/Pages/default.aspx or on request from the EA's Information Governance team by calling 028 8241 1300 or emailing infogov@eani.org.uk.

What if we need further advice and guidance?

The EA's existing data protection policies and procedures are available on the 'Think Data' intranet page - https://sharepoint.eani.org.uk/resources/thinkdata/Pages/default.aspx or on request from the EA's Information Governance team by calling 028 8241 1300 or emailing infogov@eani.org.uk. The Authority's Information Governance team is also available to advise and assist in this respect.

If you require further advice and guidance you can call 028 8241 1300 or email infogov@eani.org.uk.

Is there any advice and guidance for school based staff?

Yes. There is advice and guidance on data protection for school based staff available on the COVID-19 (Coronavirus) webpage on the EA's website (COVID-

19 Questions and Answers - https://www.eani.org.uk/covid-19-questions-and-answers)