COVID-19 Data Protection FAQs

Newsletter

Date/Version : 01 April 2020

The aim of this newsletter is to address some Frequently Asked Questions that the Data Protection Team are encountering.

This advice should be read in conjunction with the guidance given by:

- DfE regarding Safeguarding ›
- Government, regarding COVID-19 ›
- Information Commissioner's Office (ICO) regarding COVID-19 ›

Q: Due to the need to work remotely, we need to use new technology in a way we have never done before. Is there anything we need to complete before we do this?

If you are about to embark on a new process, procedure or technology, then the school should consider if a **Data Protection Impact Assessment (DPIA) is required** before you go ahead.

A DPIA is a risk assessment looking at:

- what you are going to be doing
- what data you will need
- how that data will be affected
- what can go wrong and
- how you are going to try and avoid things going wrong.

This is **mandatory** under the Data Protection Act 2018, if you are processing vulnerable individuals' data (children and employees). and the ICO would ask to see your DPIA in the case of a Data Breach to see if you properly assessed the risks and took steps to prevent it from occurring.

You do not need to complete this alone. Contact your DPO and they can assist you with the paperwork.

Q: We have completed our DPIA and are about to go live with the new project. Is there anything else we need to do?

If you are processing data in a new way, then you may need to make changes/additions to your current Data Protection documents:

- **Record of Processing Activity:** This should be an accurate reflection of how your school uses data. Therefore, if what you do changes, it needs to change.

- **Advisory Notice:** Have you communicated with the data subjects the what/how/when/why regarding the use of their data and your new processes? This can help cut complaints off at the pass.
- **Privacy Notice:** If you have made changes to how you process individuals' data then you may need to update the Privacy Notice to reflect this e.g. adding a new processing activity. This is a living document which should be continually reviewed and updated in order to accurately mirror the school's procedures and processes.

Q: As we are now dealing with COVID-19 and most staff are working remotely, do we still need to respond to Data Breaches, Subject Access Requests (SARs) and Freedom of Information Requests (FOIs)?

Yes, these are a 365-days-a-year requirement and systems still need to be in place in order to report, pick up and handle Data Breaches, SARs and FOIs.

The ICO have advised that while they cannot officially change legislation timeframes, consideration will be given if responses are delayed due to the need to shift resources away from BAU matters. However, you must still acknowledge requests/breaches and set expectation levels by communicating to data subjects regarding delays.

Consider the following:

- Can staff/do they know to report breaches, SAR's, FOI's remotely?
- Have you advised Data Subjects that the school is not running at full capacity but how they can still get in contact with you e.g. message on your website?
- Are people monitoring your office/info mailbox and able to pick up requests?
- Do they know who to forward them to and are redundancies built in if key staff are ill?

Q: We want staff to be monitoring students' engagement with work. Can they start emailing parents directly?

Yes, this is something that a number of schools already do. Parents have the email address for members of staff and can communicate with them about specific elements. However, there are some considerations:

- **Pandora's Box:** Once this occurs, it cannot be undone, parents will have your email address and potentially full name. Therefore, you may not want teachers to use their normal email accounts.
- **Generic Accounts:** Instead you can use Year1@, Admission@, SLT@, allowing staff to communicate with greater anonymity.
- **Shared Accounts:** If shared accounts are being used, then each user should be aware who else uses the account. Then they can make an assessment if the conversation they are having is something they should be privy to.
- **Communication:** Before you begin direct communication, you may want to advise the parents that this will be starting and what to expect.

- **Rules and Regs:** Like anything, it is easier to work within pre-set guidelines, advising teachers of the how/what/when of conducting email conversations and also parents as well. How you expect them to behave and what the response times are i.e. non instantaneously. If you have an 'email etiquette policy' or similar document, it may be helpful to update this. Your DPO can supply a copy of the 'standard' template for use as a basis if you do not currently have such a document.
- **Signatures:** What contact details are in the email signature and do you want people to have them e.g. direct dials and email addresses.

Q: We may need staff to be able to make phone calls, either to parents or to refer safeguarding concerns to the DSL or SLT. Should everyone be given a work mobile?

No, that is not necessary. All staff would not need to have a work mobile. However, it is worth equipping your DSL's and SLT with a work mobile. This can be a pay-as-you-go phone, which has limited functionality and only used for this time period. This allows key employees to be contactable at all times.

- **Number Forwarding:** If you have VoIP system, then you can forward your school's telephone numbers to a different device. Therefore, a personal device could be used for a limited time to receive work calls. If you don't have this functionality built in, then you can use a company like this ›*
- **Number obscuring:** Dial 141 before the number you are dialling. 'Number withheld' will be displayed to the receiving party. Therefore, staff could call a DSL (on their work mobile) or a parent without revealing their personal numbers. There are also ways to set phones up to obscure the number every time, so staff don't need to remember to do this each time they make a call. See this page (wikihow) for detailed instructions › *

Q: We want staff to be able to contact each other through more channels then just email. Can we use WhatsApp?

No, do not use WhatsApp. It may have end-to-end encryption, but its T&C's specifically state it should not be used for business purposes. In addition, it is US based, linked with Facebook and your ability to utilise your Data Rights (i.e. Access) would be limited, if not non-existent.

If you wish to use a chat function, then there is:

- Microsoft Teams ›*
- Guild App ›*
- Google Classroom ›*

*** Clicking on these links will take you to an external site. The inclusion of these links in no way constitutes a recommendation of the services or information provided and we cannot take responsibility for any pages maintained by external providers. Please use your own judgement and be especially wary of any service which asks you to pay.**

Q: We are using new remote communication tools to provide education. Do we need to ask consent from the parents or pupils before proceeding?

No, not in terms of Data Protection. The 'consent' lawful basis should only be used if individuals have real choice. If this is the **mandatory way** in which the school is going to **provide education to pupils**, there is no real choice and therefore the 'Public Task' lawful basis should be used.

If it is not mandatory, and individuals need to **download an app or register** to use the service, then this can be used as a form of consent. If they don't download or register, they have not consented and will not be using the service.

However, we always recommend communicating with the data subjects that you are proposing to make a change and advising them whether it is mandatory.

Q: How much paper can we take home with us?

As little as possible. Unlike at school where you have filing cabinets and locked offices, most homes do not have securely lockable storage and, in addition, there can be well-meaning individuals who pick up, move or read items left on display. This means the **risk of items being accidentally lost**, or **inappropriately disclosed is much higher**.

Try to **replicate as much as possible electronically**, using Word templates, remote log in and scanning to folders. If there are some tasks which just can't be conducted without paper, then a **secure storage area** needs to be found (lockable preferably) and **a logging system** created, to count in and out items from school premises so lost items can be quickly identified.

Also advise staff to **treat paper like a computer screen**, i.e. to remember that if you are not there, anyone can do anything to or with it. Therefore, do as much as possible to make it secure when you leave it e.g. **turning it over, putting it in a folder or putting it in a drawer**. The more interesting something looks, the more likely someone will read it.

Q: As the majority of our staff are now working from home, should we update our User Agreements and Code of Conduct to reflect this?

Yes, your old agreements may now be outmoded and not reflect the new issues and challenges that staff, and the school, will face.

Creating a **specific "Working from Home Agreement"** can both be a helpful guide to staff on what they should and should not be doing. Additionally, it can be an insurance policy for the school to show that they have told staff what is acceptable, if something was to go wrong. Your DPO can help with a template Working from Home Agreement, but in general they should include:

- Whether to use Personal or Work Devices – Secure Schools is an excellent resource on making personal devices secure.
- **Remote access arrangements**

- How to **communicate with colleagues and parents**
- How to **refer Data Breaches/Safeguarding/Subject Access Requests** etc
- **Data security advice**

Q: We need to have our IT supplier onsite to back-up the system, should we continue to do this?

Yes, if you need IT to be physically present in order to perform a backup of the system. **It is vital that this continues when the school is set up to work more remotely**. If the system **were to crash and information lost**, then this could **count as a Data Breach**. This of course should be done whilst observing social distancing guidance.

In general, **staff should be reminded of how an accidentally deleted file can be restored**, especially if they will need to contact your IT support themselves within a strict timeframe.

Q: The DfE has advised us that they will be using Edenred as their official supplier of PPG vouchers. Can we enter parents' email addresses into the Edenred portal so they can send the vouchers straight to the parents and not via the school as an intermediary?

Yes, if you do not want to forward on the vouchers to the parents then you can share the contact details with Edenred.

- This can be done under the **'Public Task' lawful basis**
- A copy of the **Edenred user agreement** should be saved alongside the **other contracts and user agreements** you hold.
- The sharing of this information should **be recorded in your Record of Processing Activity**
- **Before anything is sent** to the parents, it is recommended that you contact them all (through a Bcc email and **advise them who Edenred is and why they should expect an email from them**. It would be a good idea to also **include a copy of their Privacy Notice**.

Q: We are now working different hours and not monitoring shared mailboxes as much. How can we advise people of this?

Yes, being as clear and transparent with your Data subjects is always a good idea. If **your shared mailbox will not be as regularly monitored or your staff are working different hours**, then either **an out of office or auto response should be set up to explain what the working or monitoring hours are**.

Q: We want to increase the remote interaction that staff have with each other and/or with pupils - will this automatically breach data protection?

No, remote interactions will **not automatically breach Data Protection legislation**. However, like safeguarding, the correct processes need to be followed otherwise it could lead to issues.

Whether you wish to:

- Host virtual lessons using Zoom, Microsoft Teams, Google Meet or Skype
- Share Videos on your Website, Twitter or Facebook
- Narrate Slideshows

These can all be done, but need to be done correctly including:

- Undertaking due diligence on providers
- Adding activities to your Record of Processing Activity (selecting the correct Lawful Basis)
- Advising Data Subjects, through your Privacy Notices or sending out notifications
- Adding to your Data Retention Schedule
- Setting up guidance and user agreements
- Reviewing and Data Processing Agreements and contracts

Remember to check before using whether the service or app specifies that it should not be used for business purposes, or has a user age limit (e.g. YouTube may not be useful for most schools as users are supposed to be over 13 to have their own account and subscribe to channels.)

Before setting out, discuss your plans with your DPO and they can help ensure compliance.

Q: We want to use Zoom, but we hear that there are privacy and security risks with it. What is the situation?

A: Zoom is an American company who are experiencing a rapid, worldwide expansion to its original business model, so it is still catching up with the added workload and scrutiny. In addition, it is a tool which was not designed for discussing confidential topics or hosting teacher and pupil interactions, therefore trying to use it that way may cause issues without putting in procedures and protocols in place.

Privacy: Zoom is American; therefore, its servers are based in the US and would not be directly governed by the ICO. They do partake in data sharing with key selected partners. They have recently advised that they are planning to review this. This should be taken in consideration.

Security: Zoom has just amended their meetings so that a password is required to join a meeting which can only help to increase security. There are also number of other measures which can be adopted.

- Use a new meeting room each time (ie. don't use the personal meeting ID)
- Password protect your meetings and send the passwords in a separate communication.
- Don't allow attendees to join before host

- Mute attendees on joining
- Turn screen sharing off
- Set up a 'waiting room'
- Lock your meeting room after you have started
- Don't publicise your meeting's link on social media
- Don't share the screenshot of everyone, especially when it shows the meeting ID
- Try to have someone whose job it is to 'manage the room' and focus just on doing that.
- Have a user agreement which helps guide your pupils and staff – taking into account the DfE's updated Covid-19 safeguarding guidance.

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 ›