hackney success in the making

Appointing your Data Protection Officer (DPO)

March 2018

Hackney

hackney learning trust

Control Sheet: Data Protection Officer			
Reference:	**n/a**		
Date produced:	27 March 2018	**Status:**	Final
Valid until:	Revisions to current GDPR guidance; Annual Review from 1 March 2019		
Short description/ notes:	With implementation of GDPR from May 2018, HLT has developed a framework of **8 Key Tasks** for schools to complete to ensure your compliance. This Guidance Note contains guidance for the first Key Task – Appointing a DPO.		
Restrictions on use:	1. For internal use within Hackney Learning Trust and London Borough of Hackney maintained schools, academies & free schools. 2. Do not distribute without permission from the person authorising use.		
Reporting cycle:	Updated as new guidance becomes available		
Next report due:	TBC		
Report location:	▪ Strategy, Policy & Governance networked folders; file name: 01 GDPR Guidance - Appointing a DPO FINAL DRAFT 180327 ▪ Services for Schools website		
Supplied by:	Sean O'Regan	**Role:**	DPA & FOI Officer
Checked by:	Hilary Smith	**Role:**	Head of Strategy, Policy & Governance
Authorised for use by:	Frank O'Donoghue	**Role:**	Head of Business Services
Updates in this briefing are included for the following areas of the data matrix:			
N/a at this point			

1. Appointing a Data Protection Officer (DPO)

As maintained schools and academies are public authorities you **do** need to appoint a DPO to ensure compliance with the GDPR.

The full text of the GDPR and supporting articles are available on line – go to http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN

2. What does a DPO do?

The DPO takes an advisory and monitoring role and should actively guide your school's ongoing efforts to comply with the GDPR. It is still the school's responsibility as a data controller to ensure compliance, so the DPO will not be held personally responsible if anything goes wrong.

The main tasks of a DPO are defined in Article 39 of the GDPR:

1. To inform and advise the organisation and its employees about their obligations under the GDPR.
2. To monitor compliance with the GDPR, including awareness raising and training of staff involved in the processing operations.
3. To respond to Subject Access Requests and to report any breaches of data security if required.
4. To be the first point of contact for the ICO and for individuals whose data is processed (pupils, employees etc). To cooperate with the ICO if/when required.
5. To provide advice with regard to data protection impact assessments

As the first two points above show, the DPO role is largely advisory. Their main role is to raise awareness of data protection issues and be a data protection champion within the school. The DPO makes things happen and advises on how they should be done, but will not necessarily complete those tasks personally.

To clarify, the Key Tasks identified for ensuring compliance with the GDPR in the HLT Framework (please see Introductory Note) will likely be completed by various people and are not the sole responsibility of the DPO.

The fifth point above is closely linked to points one and two. Article 35 requires data controllers to undertake data protection impact assessments (DPIA) where a type of processing (in particular using new technologies) is likely to result in a high risk to the rights and freedoms of data subjects. This means that if your school is considering processing personal data in a new way, in particular using new technology or applications, the DPO shall provide advice and guidance on what the data protection risks may be, and what you can do to manage those risks. HLT will issue separate guidance on DPIAs for schools to follow at a later date.

DPOs may occasionally be required to commit a significant amount of time and effort if the school receives a Subject Access Request or if a data breach occurs and requires investigation and resolution. However, ultimately the responsibility of ensuring compliance with GDPR lies with the school as a data controller and with all of its staff who process personal data in performing their main duties.

3. Who should schools appoint as DPO?

Your DPO can be a school employee or a school governor (though not the Chair of the governing body). Alternatively, you can engage a DPO service from an external provider.

The appointed DPO can work across various schools. This could be schools in a federation or a less formal arrangement if a group of schools agree to share a DPO. The DPO should not be anyone employed on a short or fixed term contract. Continuity and familiarity with how your school processes personal data and an ability to exert influence across the school workforce will be key to performing the DPO role to a high standard.

The DPO will report to the highest management level of your school, i.e. the Chair of Governing body or the trust board. They must be allowed to perform their tasks independently and should not be unduly influenced by senior school leaders in how they go about their duties as DPO.

In practise, this means the DPO must be able to identify best practise and guide the school in fulfilling its data protection responsibilities without direction, reporting to the Chair of the governing body/trust board if required.

Article 37(5) of GDPR states;

> *"The data protection officer shall be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfil the tasks referred to in Article 39."*

While GDPR requires that any DPO should have professional experience and knowledge of data protection law it does not specify precise credentials or qualifications. The required level of expertise is not strictly defined but it must be commensurate with the sensitivity, complexity and amount of data an organisation processes.

Schools of course process some highly sensitive personal data, however, the processing activities are relatively straightforward and small in scale compared to larger private companies which utilise automated decision making processes or share data outside of Europe. School DPOs will be principally concerned with keeping data secure and ensuring all data processing is fair, lawful and transparent.

So, given the relatively uncomplicated nature of the majority of data processing in schools, a member of staff with previous experience of data protection matters can enhance their knowledge through training and research to perform the role within a school to the required standard. A member of staff lacking prior experience could also be brought up to speed with some good training.

The Article 29 Guidance also states that the ability to perform the role of DPO;

> *"… should be interpreted as both referring to their personal qualities and knowledge, but also their position in the organisation."*

If you are appointing internally it should be an individual who is confident and well placed within the school to enact any required changes.

Article 38(6) specifies they must be able to do so while avoiding any potential conflict of interest in their other duties. The EU Article 29 Working Party has published some guidance which includes specific reference to avoiding conflicts of interest, which states;

> *"….the DPO cannot hold a position within the organisation that leads him or her to determine the purposes and the means of the processing of personal data. Due to the specific organisational structure in each organisation, this has to be considered case by case"*

By and large there should be few examples of such conflicts of interest in a school setting. It is helpful to first of all think about what would constitute a conflict of interests. Much of the data processing activities in a school relate to its statutory duties of educating and safeguarding its pupils or reporting to government agencies about its pupils or workforce. These data processing activities do not involve decision making as you are complying with legal obligations or fulfilling the school's core functions in accordance with established procedures. The purposes for processing personal data in schools are, on the whole, pre-determined.

The issue of conflicts of interest is also closely linked to the requirement to act independently and impartially. A significant potential source of conflict in a school context may arise from the responsibility to respond to subject access requests and report data breaches. A conflict could arise if the personal data relates to actions taken by the DPO in their core role as a line manager, or an error on their part leading to a data breach. Such risks can be mitigated by appointing a DPO with the necessary personal qualities referred to in the Article 29 Group guidance. A DPO with integrity and high professional ethics

would be able to focus on enabling compliance with the GDPR regardless of any implications for them personally.

Another example of potential conflict would be if the DPO made a decision, as part of their core duties, which resulted in personal data being collected or used for a new purpose. If the DPO is making that decision personally, they cannot review that decision from a data protection perspective and provide independent advice and guidance. One way to think about the advisory and monitoring role of the DPO is that you cannot mark your own homework. The best way to avoid such conflicts is to ensure such decisions are ultimately made either collectively or by a senior school leader who is not the DPO.

A good place to start when considering your appointment would be to identify and explain what conflicts of interest might arise from having a specific staff member as DPO. Some types of staff you might consider;

3.1. Business Managers

Although Business Managers may process personal data in various ways, data processing activities relating to the management of the school workforce, educating and supporting its pupils and reporting for the school census and school workforce census are not subject to decision making processes that determine the purposes of the data processing. These data processing activities relate to core public interest functions or specific legal obligations.

Decisions about information management systems and applications that process personal data, e.g. SIMS or a texting or emailing service for sending notifications to parents would not necessarily constitute making decisions that '*determine the means of the processing of personal data'.* If such decisions are ultimately made collectively, i.e. subject to governing body approval or are referred to the Headteacher, then the Business Manager does not make the decision that determines the means of processing and there is not a conflict of interests.

When discussing the need to avoid potential conflicts of interest the Article 29 Working Group guidance does acknowledge that *"Due to the specific organisational structure in each organisation, this has to be considered case by case".* The ICO has also avoided specifying job titles that would prohibit people from performing the DPO role in schools.

Of all managers in schools, Business Managers are well placed to take on the role of DPO and currently predominantly manage their school's responsibilities under the current Data Protection Act. Provided you can take steps to avoid conflicts of interests, HLT would advise schools consider appointing the Business Manager as DPO.

3.2. Deputy Heads and other Senior Leaders

With all of the above in mind, the appointment of senior leaders should not be discounted entirely if the individual is the best fit in terms of knowledge of data protection and having the capacity to perform the role effectively. Such a member of staff could also work closely with a Business Manager providing support and an independent view on data protection matters.

Their day to day duties would not involve making decisions about the purposes and means of processing personal data. While aspects of their work may be called into question as part of a subject access request, e.g. a parent appealing an exclusion or how a pupil's behaviour is managed in class, any risk of a conflict of interest could be mitigated by appointing an individual with the required personal qualities.

Deputy Heads and other Senior Leaders are likely to require more training than Business Managers as they are likely to have less prior experience or knowledge of data protection.

3.3. Appointing externally

There are organisations that will provide this service for a fee, however, there are no guarantees as to how dedicated or focussed on your school this service will be.

A significant benefit of appointing internally is that, once that individual has received training and developed their knowledge of data protection, they are well placed to deal with any routine matters such as maintaining the Information Asset Register, or unexpected matters such as subject access requests or data breaches quickly and efficiently, at no additional cost to school finances.

Internal DPOs will also be familiar with the day to day operation of the school as well as staffing structures and organisation, which can help to understand how to implement GDPR requirements efficiently & effectively.

Given the above, we believe that the benefits of appointing an internal DPO outweigh those of an external DPO.

3.4. Governors

One option some schools have indicated would be viable is appointing a school governor. A school governor with legal experience could be desirable. A school governor would report directly to senior school leaders and be able operate independently while having access to data if required (e.g. in responding to a subject access request).

A governor with relevant skills, knowledge and (more crucially) the time to perform the role of DPO would need to be able to provide day to day operational support which could be in conflict with possessing the right blend of understanding, seniority and independence to perform the role of DPO to a high standard.

The DPO's role in responding to Subject Access Requests or data breaches within clearly specified timeframes also highlights the difficulties that appointing someone who is not a school employee may bring. Sometimes a quick response or a significant time commitment may be required, schools should consider whether appointing an individual who is not a school employee will guarantee this.

Given the above, we believe that the operational difficulties and potential conflicts of interest outweigh any benefits of this option.

4. Summary

HLT is of the view that the work to ensure compliance by 25 May 2018, and the ongoing monitoring and advisory work of the DPO after this date, does not require schools to engage third party service providers. This is of course each school's choice to make, however, HLT will provide ad hoc support as we have done under the existing legislation over the years to schools which elect to appoint a DPO from among the school's existing staff. Your legal services provider may also be able to provide additional advice and support.

If you are considering appointing a DPO from school staff, the key is to ensure that the person appointed has the right qualities. The number of potential DPOs will likely be low if the appointment process is guided solely by avoiding potential conflicts of interest. Knowledge and experience, personal qualities and ability to guide the school as an organisation should all be factors in any appointment decision.

As we have seen, the types of conflict of interest that can arise in the context of data protection varies depending on the type of organisation. Organisations involved in more complicated data processing activities which change over time are more likely to identify potential conflicts of interests as their employees make decisions that directly affect why and how the process data.

In a nutshell, a DPO must never be tasked with deciding what personal data their organisation collects or why and how it is used as part of their core role. In a school context, the purposes for processing

personal data are largely dictated by core public interest functions (e.g. educating and safeguarding pupils) or specific legal obligations (e.g. school census).

Think about what personal data your school collects and how it is used. Who decides this? Is it the government (e.g. school census?) or something the school must do to function (e.g. maintaining pupil records)? Likewise with decisions as to how (or the means by which) personal data is processed. Who makes these decisions? Are they made collectively at Governing Body level or ultimately referred to the Headteacher? Who would be best placed to advise the school as a data controller as to what the data protection implications might be?

Once you have made a decision as to who is appointed this should be documented, with any concerns about any conflicts of interests weighed against the suitability of the individual if required. While HLT can provide some initial support on these issues, the more experienced and knowledgeable the DPO is on data protection matters, the easier it will be for the school to embed into its day to day operations and ethos, so ensuring compliance with GDPR requirements.