hackney success in the making

4. Reviewing arrangements with data processors

May 2018

Hackney

hackney learning trust

Control Sheet: Reviewing Arrangements with Data Processors			
Reference:	**n/a**		
Date produced:	23/05/2018	**Status:**	Final Draft
Valid until:	Revisions to current GDPR guidance; Annual Review from 1 May 2019		
Short description/ notes:	With the implementation of GDPR from 25 May 2018, HLT has developed a framework of **8 Key Tasks** for schools to complete to ensure compliance. This briefing note addresses what schools must do to ensure their arrangements with third party data processors are GDPR compliant.		
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 Hackney Learning Trust.		
Reporting cycle:	Updated as new guidance becomes available		
Next report due:	TBC		
Report location:	▪ Strategy, Policy & Governance networked folders – 04 - Reviewing arrangements with third party data processors V180511 ▪ Services for Schools website – https://www.hackneyservicesforschools.co.uk/extranet/gdpr		
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. Introduction

1.1. Having completed your Information Asset Register (IAR) you will have identified the relationships your school has with any third parties. Now is the time to review the arrangements you have with these third parties to ensure any activities involving your school's personal data are compliant with the GDPR and that your data subjects' rights are protected.

1.2. The GDPR states that whenever a data controller uses a third party to process its personal data (a data processor) there needs to be a written contract in place.

1.3. These contracts must include certain specific terms designed to ensure that the data processing undertaken by data processors meets all the requirements of the GDPR. The GDPR allows for standard contractual clauses from the EU Commission or a supervisory authority (such as the ICO) to be used in contracts, however, none have been published so far.

1.4. The Crown Commercial Service has issued an action note titled 'Procurement Policy Note (PPN) – Changes to Data Protection Legislation & General Data Protection Regulation' which provides clear guidance and recommendations for public authorities which are data controllers;

1.5. The Information Commissioner's Office has also published very helpful guidance on contracts and liabilities between controllers and processors;

1.6. This guidance considers the recommendations of the above and addresses what schools need to do as data controllers. However, we would highly recommend that schools consult the ICO guidance above with regard to contracts and liabilities where personal data is concerned.

1.7. This guidance does not relate to data processing activities involving Hackney Learning Trust. Information sharing between schools and HLT relating to statutory and public interest tasks will be addressed in an Information Sharing Agreement to be issued by HLT as part of the Council's GDPR compliance work. Data processing activities relating to HLT's traded services will be addressed in revised Terms and Conditions to be listed on the Services for Schools website.

2. Timing

2.1. Schools must begin to apply the provisions of this guidance immediately to ensure any required contract amendments take effect from 25 May 2018 or as soon as possible thereafter. Schools must also ensure the new provisions are applied to all new relevant contracts awarded after 25 May 2018.

3. Actions to take

3.1. Schools should:

- Identify any existing contracts involving the processing of personal data which will be in place after 25 May 2018. Examples of third party data processors you may engage would be payroll providers and providers of software services with whom you have a software maintenance agreement, such as Tucasi, SISRA Analytics, Parent Pay/Parent Mail, Group Call Emerge, Contact Group, or any other application that involves use of personal data.
- Many larger providers will have already contacted you regarding their compliance with GDPR and changes to terms and conditions, but if you have not heard from a provider the school should take the initiative. Write to all identified data processors who have not changed their contract terms and conditions notifying them that changes will need to be made to the contracts to bring them in line with the GDPR (draft letter attached as Appendix A).
- Update relevant contract terms and conditions by issuing contract variations if the school issued the contract, or request this from the provider if they issued the contract. Updated contracts should include the GDPR clauses recommended by the Crown Procurement Service in their action note (Appendix B) and a processing schedule (template and guidance text attached as Appendix C).
- Undertake due diligence of all new data processors before entering into contracts to ensure they can implement the appropriate technical and organisational measures to keep the school's personal data secure to ensure compliance with the GDPR.

- Ensure all new contracts involving the processing of personal data include GDPR clauses and a detailed processing schedule.

4. Data Controllers and Data Processors

4.1. The definitions of 'Controllers' and 'Processors' under the GDPR are broadly the same as under the existing DPA.

- A data controller decides the purposes and means of data processing; and
- A data processor processes personal data on behalf of the data controller and in accordance with conditions imposed by the data controller.

4.2. Sometimes there may be a further Sub-processor(s) if the data processor uses another third party organisation to carry out any data processing activities on behalf of the school. The same data protection obligations set out in the contract between the school and the processor must be imposed on any sub-processor(s) by way of a contract. Contracts should oblige the processor to notify the controller if there are any sub-processors involved.

5. Contracts and Liabilities

5.1. Schools can use contracts to ensure they retain control over the purposes and means of the data processing and to clearly advise the third party about what is expected of them as data processors.

5.2. Under the DPA, data controllers are ultimately responsible for keeping the data secure and ensuring it is processed in accordance with the data protection principles, i.e. the data controller is responsible for any breaches resulting from a failure to comply with the DPA by the data processor. Under the GDPR, data processors now face direct legal obligations and can be fined by the Information Commissioner's Office. Both data controllers and data processors can face claims for compensation where they have not complied with their obligations under the GDPR.

5.3. Therefore, schools should never accept any liability clauses where data processors are indemnified against fines or claims under the GDPR. The legal penalty regime has been extended under the GDPR to include data processors to ensure better performance and enhanced protection of personal data. So, to accept any conditions intended to indemnify data processors for any fines or court claims would undermine the principles of the GDPR.

5.4. Data processors may incur costs as a result of ensuring their compliance with the GDPR, for example if they have to upgrade their ICT network security arrangements or procure a new email encryption service. However, such costs are inevitable for any data processors who wish to operate within the EU and should not be a factor in any negotiations about what your school pays for their services. Data processors should be expected to manage their own costs relating to compliance with the GDPR, so be mindful of any organisations that may try to impose contract price increases as a result of work associated with compliance with the GDPR.

6. Risks of Non-Compliance

6.1. Schools found not to be GDPR compliant by 25 May 2018 will be in breach of the regulations and at risk of being fined or having an enforcement order issued by the Information Commissioner's Office. As has been stated in previous Guidance Notes, the ICO are not looking to impose financial penalties or enforcement orders on schools. However, out of date contractual arrangements can expose your school to unnecessary risk and are a very clear sign of an organisation not being mindful of data protection regulations.

7. Joint Controllers

7.1. There may be instances where schools act as joint controllers with other organisations. In these cases, the GDPR states that joint controllers have to have a transparent 'arrangement' between them which must 'duly reflect the respective roles and relationships of the joint controllers vis-à-vis the data subjects'.

7.2. An example of this type of arrangement would be schools and local authorities in relation to school admissions data. Both schools and the local authority determine the purposes and means of the data processing as each party works together to ensure school placements are allocated.

7.3. Admissions data, and data sharing between Hackney schools and HLT in the wider sense, will all be addressed in an Information Sharing Agreement to be issued by HLT as part of the Council's GDPR compliance work.

Appendix A – Letter to third parties processing personal data

[insert draft text, amending as appropriate]

New data protection legislation is due to come into force on 25 May 2018, which aims to enhance the protection afforded the privacy of all EU citizens and prevent data breaches. It will apply to any individual, public or private organisation processing personal data.

Established key principles of data privacy will remain relevant in the new data protection legislation but there are also a number of changes that will affect commercial arrangements, both new and existing, with data processors. The new General Data Protection Regulation specify that any processing of personal data, by a data processor, should be governed by a contract with certain provisions included.

We have identified a contract between **[insert name of school]** and **[insert name of data processor]** involving processing personal data, and which will be in place after 25 May 2018, that requires updating to bring it in line with the new Regulation.

This will involve updating contract terms and ensuring specifications reflect the roles and responsibilities between the school and the **[insert name of data processor]** as required by the new Regulation.

In addition, we will be updating our procurement documentation to reflect the new Regulation for contracts to be awarded on or after 25 May 2018.

Any organisation required to comply with the new data protection legislation may incur costs in doing so, especially where new systems or processes are required. However, these costs are attributable to conducting business in the EU, and not supplying the UK public sector. We expect all data processors to manage their own costs in relation to compliance with the Regulation.

We will not accept liability clauses where you are indemnified against fines under Regulation as indemnifying data processors in respect of any fines or court claims would undermine the principles of the Regulation, because the legal penalty regime has been extended directly to data processors to ensure better performance and enhanced protection for personal data.

The Crown Commercial Service has issued an action note titled 'Procurement Policy Note (PPN) – Changes to Data Protection Legislation & General Data Protection Regulation' which provides clear guidance and recommendations for public authorities which are data controllers;

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/674575/FINAL_PUBLISHED_GDPR_PPN_03-17.docx.pdf

Please note that any contracts between **[insert name of school]** and **[insert name of data processor]** will need to reflect these recommendations, specifically, all contracts must include the recommended clauses listed as Annex A and a detailed data schedule.

Please contact **[insert name and email address/phone number of school DPO]** to discuss how we can ensure our data processing activities are fully compliant with the GDPR and how we can update our contractual documentation to reflect this.

If you would like to know more about the upcoming changes, the Information Commissioner's Office is a useful source of information on the new regulations (https://ico.org.uk/media/about-the-ico/consultations/2014789/draft-gdpr-contracts-guidance-v1-for-consultation-september-2017.pdf).

Appendix B: Generic Standard GDPR Clauses Recommended by the Crown Commercial Service

1. DATA PROTECTION

1.1 The Parties acknowledge that for the purposes of the Data Protection Legislation, the Customer is the Controller and the Contractor is the Processor. The only processing that the Contractor is authorised to do is listed in Schedule [X] by the Customer and may not be determined by the Contractor.

1.2 The Contractor shall notify the Customer immediately if it considers that any of the Customer's instructions infringe the Data Protection Legislation.

1.3 The Contractor shall provide all reasonable assistance to the Customer in the preparation of any Data Protection Impact Assessment prior to commencing any processing. Such assistance may, at the discretion of the Customer, include:

(a) a systematic description of the envisaged processing operations and the purpose of the processing;
(b) an assessment of the necessity and proportionality of the processing operations in relation to the Services;
(c) an assessment of the risks to the rights and freedoms of Data Subjects; and
(d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of Personal Data.

1.4 The Contractor shall, in relation to any Personal Data processed in connection with its obligations under this Agreement:

(a) process that Personal Data only in accordance with Schedule [X], unless the Contractor is required to do otherwise by Law. If it is so required the Contractor shall promptly notify the Customer before processing the Personal Data unless prohibited by Law;
(b) ensure that it has in place Protective Measures, which have been reviewed and approved by the Customer as appropriate to protect against a Data Loss Event having taken account of the:

(i) nature of the data to be protected;
(ii) harm that might result from a Data Loss Event;
(iii) state of technological development; and
(iv) cost of implementing any measures;
(c) ensure that :
(i) the Contractor Personnel do not process Personal Data except in accordance with this Agreement (and in particular Schedule X);
(ii) it takes all reasonable steps to ensure the reliability and integrity of any Contractor Personnel who have access to the Personal Data and ensure that they:

(A) are aware of and comply with the Contractor's duties under this clause;
(B) are subject to appropriate confidentiality undertakings with the Contractor or any Sub-processor;
(C) are informed of the confidential nature of the Personal Data and do not publish, disclose or divulge any of the Personal Data to any third Party unless directed in writing to do so by the Customer or as otherwise permitted by this Agreement; and
(D) have undergone adequate training in the use, care, protection and handling of Personal Data; and

(d) not transfer Personal Data outside of the EU unless the prior written consent of the Customer has been obtained and the following conditions are fulfilled:

(i) the Customer or the Contractor has provided appropriate safeguards in relation to the transfer (whether in accordance with GDPR Article 46 or LED Article 37) as determined by the Customer;
(ii) the Data Subject has enforceable rights and effective legal remedies;
(iii) the Contractor complies with its obligations under the Data Protection Legislation by providing an adequate level of protection to any Personal Data that is transferred (or, if it is not so bound, uses its best endeavours to assist the Customer in meeting its obligations); and
(iv) the Contractor complies with any reasonable instructions notified to it in advance by the Customer with respect to the processing of the Personal Data;

(e) at the written direction of the Customer, delete or return Personal Data (and any copies of it) to the Customer on termination of the Agreement unless the Contractor is required by Law to retain the Personal Data.

1.5 Subject to clause 1.6, the Contractor shall notify the Customer immediately if it:

(a) receives a Data Subject Access Request (or purported Data Subject Access Request);
(b) receives a request to rectify, block or erase any Personal Data;
(c) receives any other request, complaint or communication relating to either Party's obligations under the Data Protection Legislation;
(d) receives any communication from the Information Commissioner or any other regulatory authority in connection with Personal Data processed under this Agreement;
(e) receives a request from any third Party for disclosure of Personal Data where compliance with such request is required or purported to be required by Law; or
(f) becomes aware of a Data Loss Event.

1.6 The Contractor's obligation to notify under clause 1.5 shall include the provision of further information to the Customer in phases, as details become available.

1.7 Taking into account the nature of the processing, the Contractor shall provide the Customer with full assistance in relation to either Party's obligations under Data Protection Legislation and any complaint, communication or request made under clause 1.5 (and insofar as possible within the timescales reasonably required by the Customer) including by promptly providing:

(a) the Customer with full details and copies of the complaint, communication or request;
(b) such assistance as is reasonably requested by the Customer to enable the Customer to comply with a Data Subject Access Request within the relevant timescales set out in the Data Protection Legislation;
(c) the Customer, at its request, with any Personal Data it holds in relation to a Data Subject;
(d) assistance as requested by the Customer following any Data Loss Event;
(e) assistance as requested by the Customer with respect to any request from the Information Commissioner's Office, or any consultation by the Customer with the Information Commissioner's Office.

1.8 The Contractor shall maintain complete and accurate records and information to demonstrate its compliance with this clause. This requirement does not apply where the Contractor employs fewer than 250 staff, unless:

(a) the Customer determines that the processing is not occasional;
(b) the Customer determines the processing includes special categories of data as referred to in Article 9(1) of the GDPR or Personal Data relating to criminal convictions and offences referred to in Article 10 of the GDPR; and
(c) the Customer determines that the processing is likely to result in a risk to the rights and freedoms of Data Subjects.

1.9 The Contractor shall allow for audits of its Data Processing activity by the Customer or the Customer's designated auditor.

1.10 The Contractor shall designate a data protection officer if required by the Data Protection Legislation.

1.11 Before allowing any Sub-processor to process any Personal Data related to this Agreement, the Contractor must:

(a) notify the Customer in writing of the intended Sub-processor and processing;
(b) obtain the written consent of the Customer;
(c) enter into a written agreement with the Sub-processor which give effect to the terms set out in this clause [X] such that they apply to the Sub-processor; and
(d) provide the Customer with such information regarding the Sub-processor as the Customer may reasonably require.

1.12 The Contractor shall remain fully liable for all acts or omissions of any Sub-processor.

1.13 The Customer may, at any time on not less than 30 Working Days' notice, revise this clause by replacing it with any applicable controller to processor standard clauses or similar terms forming part of an applicable certification scheme (which shall apply when incorporated by attachment to this Agreement).

1.14 The Parties agree to take account of any guidance issued by the Information Commissioner's Office. The Customer may on not less than 30 Working Days' notice to the Contractor amend this agreement to ensure that it complies with any guidance issued by the Information Commissioner's Office.

Appendix C – example specification & service delivery schedule (to be added as an appendix to contracts with Data Processors).

This example was drafted using the example of a schedule to a contract between a school and provider of a reading support application which requires pupils and parents to sign up and log in to. It is intended as general guidance in terms of the level of detail you need to go into, however, more complicated data processing activities will require a commensurate level of detail;

Schedule [X] Processing, Personal Data and Data Subjects

1. The parties acknowledge that for the purposes of the Data Protection Legislation, the Customer is the Controller and the Contractor is the Processor. The only processing that the Contractor is authorised to do is listed in Schedule [X] by the Customer and may not be determined by the Contractor.
2. The Contractor shall comply with any further written instructions with respect to processing by the Customer
3. Any such further instructions shall be incorporated into this Schedule.

Description	Details
Subject matter of the processing	The processing is undertaken for the provision of a reading skills development programme to track and support pupil progress in literacy as part of the School's public task of supporting, monitoring and reporting on pupil learning.
Duration of the processing	From commencement of contract to its termination.
Nature and purposes of the processing	The School carries out tasks that are in the public interest to provide education to children and support their learning and development. The School will engage the Contractor to provide an online reading support programme designed to support, monitor and track each pupil's progress. The Contractor will require access to limited personal data about the Customer's data subjects and their parents in order to support the development of their reading and writing skills. Information will flow both ways between the School and Contractor and will be accessible to parents of pupils using the service. The Contractor will abide by the data security and procedural data protection standards imposed by the Contract. [Consent for information to be held will be sought by the Customer at the start of the process, when pupils start Year 3. Access to the online portal will be by username and password which will be sent directly to the teacher and parents of pupils using the service.]
Type of Personal Data	Information about individuals processed under the contract will include; • **Forename, Surname, DOB, Age, Gender** – For all service users (pupils in Years 3 and 4) • **Forename, Surname and email address** for teachers of service users. • **Forename, Surname and email address** for parents of service users.

Description	Details
	• **[Details of reading activities undertaken and achievements**, with dates.]
Categories of Data Subject	School staff (including teachers, volunteers and temporary workers), pupils and parents
Plan for return and destruction of the data once the processing is complete UNLESS requirement under union or member state law to preserve that type of data	The personal data will be retained until the pupil finishes using the Service. The Contractor will then delete the personal data securely Any personal data will be returned by the Contractor to the School at termination of contract at no expense to the School.