GDPR Compliance Briefing Note

2. Completing your school's Information Asset Register and Information Audit

March 2018

Control Sheet: Guidance for completing Information Asset Register			
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 on completing an Information Asset Register and Information Audit.		
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: 02 GDPR Guidance - Information Asset Register FINAL 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			

Guide to filling in your Information Asset Register

1. Why do I need an Information Asset Register

The main changes arising from GDPR are a raised focus on transparency, control and accountability. The Information Asset Register (**IAR**) is designed to help you meet these new requirements around **accountability**. Among other things, records must be kept on processing purposes, data sharing, and retention.

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.

More information about the explicit provisions within the GDPR that require you to maintain internal records of your processing activities can be found on the Information Commissioner's Office website (https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/documentation/).

The IAR will help you to map out your data processing activities and answer the following questions;

- what personal data does the school hold
- how and when is that data collected
- where and how is it stored
- is the data shared with any third parties?
- do you have a sound legal basis for processing the data?

This will in turn help you to be transparent once you have clarified all the data processing activities you are involved in and what your legal basis is. Most of your data processing activities will relate to legal obligations or be key in enabling the school to function. However, if your teachers or school office are using new apps that use personal data, now is the time to identify and document these new activities and check they are GDPR compliant.

2. What is an Information Asset Register?

'Information Asset' may seem like odd terminology, however, it is simply a way of referring to a large number of individual records grouped together by type (e.g. 'Pupil Educational Records'). The IAR is a list of your information assets including all the key information you need to know about each one.

Try to avoid dividing information assets up where possible, even if they contain varied data or are held across formats. If that information is used for a common purpose then it should be listed as one information asset.

A good example is pupil educational records. Pupil educational records will contain different types of information and be held in both physical and electronic formats. However, all of this information is used together for the common purposes of supporting the pupil's learning, providing pastoral care and monitoring/reporting on their progress.

Another example could be if you hold any apps where parent data is held (outside the SIMS system), this is an area that would be important to include.

Use terms that all school staff would easily understand when describing information assets, e.g. 'Exclusion Records'. As the IAR will be reviewed annually (at least) it must be easily comprehensible to whoever is reviewing it in the future.

It should not be overly time consuming and your IAR should not be too complicated. If it is overly complicated it will not serve its core purpose of clearly mapping out your data processing activities.

We estimate schools will identify approximately 10 different information assets following the guidance

above, however, you may choose to record things differently. Most data controllers are doing this for the first time and there is no universally acknowledged correct method. All that matters is that your IAR makes sense to people at your school and clarifies how you are processing personal data.

3. Completing your school's IAR

HLT have used the IAR being developed by the Council to provide a template IAR for schools to use. The following provides guidance on how to fill in each column of the Register.

3.1. Asset Number or ID

You may want to catalogue the information assets held by the school using a unique individual identifier to keep track of each entry onto the register – e.g., by number or some other form of index.

3.2. Name of Asset

This should be a name that will be easily recognisable to anyone who would be involved in maintaining the register. Be descriptive but not overly concerned with listing things by technical names – e.g., Pupil Educational Records; HR Staffing Records.

3.3. Department/Information Asset Owner

Who is the primary owner / manager of the information listed – e.g. employment records may be held by the Business Manager or SEND information held separately by the SENCo.

3.4. Volume

Specify how many individuals the personal data in the identified Information Asset relates to. If it is a high number of people that may be subject to change an approximate number will suffice.

3.5. How and When is the Data Collected?

Where did the data come? Was it provided by parents/families in a form? Did you receive the data from the Local Authority or another external organisation (e.g., health provider, etc) or was it generated internally (e.g., internal assessment)? It is important to note this in order to keep track of what consent was obtained at the time as to how the data will be used. It also feeds into what you need to say in your Privacy Notice in terms of what you use data for.

3.6. What personal data does the Information Asset contain?

Briefly describe what types of personal data is held in the information asset – e.g. Pupil Educational Records will contain name, D.O.B., address and contact details, health/dietary requirements etc.

3.7. Special Category Data

Does the information asset contain Special Category data (previously known as sensitive personal data)? Special Category data is any information relating to the following;

- data revealing racial or ethnic origin,
- political opinions,
- religious or philosophical beliefs,
- trade union membership, and;
- genetic data, biometric data for the purpose of uniquely identifying a natural person,
- data concerning health
- data concerning a natural person's sex life or sexual orientation

3.8. Processing Activities

Specify what the personal data in the information asset is used for.

3.9. **Legal Basis for Processing**

Article 6 of the GDPR sets out the legal bases for processing personal data. If you are processing special category data, you need to identify both a lawful basis for that processing and a special category condition for processing in compliance with Article 9. You should document both your lawful basis for processing and your special category condition so that you can demonstrate compliance and accountability.

Legal bases for processing personal data are listed in Article 6 (Lawfulness of Processing) of the GDPR;

(a) the data subject has given consent

(b) processing is necessary for the performance of a contract

(c) processing is necessary for compliance with a legal obligation

(d) processing is necessary to protect data subject's vital interests

(e) processing is necessary for the performance of a task carried out in the public interest

(f) the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks.)

It is clear from the GDPR that consent should not always be relied upon as a valid lawful basis for processing data, in particular where the data controller is a public authority. HLT would encourage schools to identify and rely on the other lawful bases of processing wherever applicable – i.e., (c) (legal obligation), (e) (public interest task) and (f) (legitimate interests wherever the data processing does not relate to the school's core functions).

Legal bases for processing Special Category (sensitive data) which schools may use are listed in Article 9 (processing of special categories of data), paragraph 2 – the relevant bases being;

(b) The processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or data subject in the field of ***employment*** *and* ***social security*** *and* ***social protection law****;*

(c) The processing is necessary to protect the ***vital interests of the data subject*** *or of another natural person where the data subject is physically or legally incapable of giving consent;*

(g) The processing is necessary for reasons of substantial ***public interest*** *and proportionate to the aim pursued.*

Statutory data processing activities such as submitting data for the school census and workforce census will fall under Articles 6(c) and 9(2)(b) respectively. Other data processing that is necessary for your school to function will fall under Articles 6(e) and 9(2)(g) (public interest).

Non-statutory data processing must be justified under another legal bases listed in Articles 6 and 9 where Special Category (sensitive) data is involved.

3.10. **Key Asset**

Is the processing activity the personal data used for a core function of the school? If yes, it is likely that your legal basis for processing will fall under articles 6(e) and 9(g).

3.11. **Format**

On what format is the data held? Is it a paper or electronic record? Or both?

3.12. **Location of Hardcopy Records**

If the personal data is held, or partly held, in hardcopy paper form what is the physical location? E.g., is it held onsite, stored offsite using a contracted provider (if so, rive details of contractor) or other offsite provision (give details & location).

3.13. **Application**

This relates to software programmes or databases in which any personal data is held, e.g. Capita One

3.14. **Access**

Who can access the Information Asset whether it be a paper file or records held on a computer? Specify which job roles will require such access.

3.15. **Security Controls**

Are there any special security controls for accessing the data within the Information Asset? Examples would be keeping paper records in a locked room or filing cabinet, or records held on a software package where passwords are strictly limited to specified school staff.

3.16. **Is the data shared with any third parties?**

Does the school share the data within the Information Asset with any third parties? Schools will share some data with Hackney Learning Trust and other agencies for statutory purposes, but may also send data elsewhere for a number of reasons. It is essential to identify this in order to ensure that information sharing is fair and lawful, that adequate information sharing agreements are in place and that the sharing is clearly described in the Privacy Notice.

3.17. **Legal Basis for Sharing**

Where you have identified that data is being shared with a third party you must identify the legal basis for sharing the data.

Most information sharing will relate to statutory functions, however, you may also engage private companies for services that involve processing personal data (e.g. a texting or mailing app for contacting parents). You must identify whether or not any non-statutory data sharing is compatible with the purpose for which it was stated the information was collected from the parents for.

For the purposes of the Register you should only refer to routine information sharing. Access to personal data may be requested by the police or other authorised agencies in relation to specific investigations, but this can be documented separately in order to keep your Register focussed on mapping data flows you know will occur.

3.18. **Information Sharing**

Some information sharing activities will be governed by an Information Sharing Agreement/Protocols. It may be the case that your contract with a third party contains specific clauses addressing data protection issues and each party's responsibilities. If you are sharing the personal data within the Information Asset with a third party, check your contracts with those third parties to ensure adequate data protection assurances are in place (please see separate guidance to be published on Contracts).

3.19. **Third Party Data Processing**

Do you have a contract in place with a third party to process any personal or sensitive data for you? (e.g. ParentMail). If yes, you should have an agreement in place setting out what the data processor can and cannot do with the personal data and their responsibilities for keeping the data secure?

3.20. **Transfer outside of UK/EU?**

The GDPR imposes restrictions on the transfer of personal data outside the European Union, to third countries or international organisations. These restrictions are in place to ensure that the level of protection of individuals afforded by the GDPR is not undermined if the data is transferred to a place

where the GDPR does not apply.

Some software programmes or databases may be hosted on servers outside the European Union. It is essential that you check this information and ensure that any such arrangements are fully covered by contracts including specific clauses and provisions stipulated by the EU Commission.

3.21. **Profiling/Automated Decision Making**

Some personal data is collected in order to feed into computer based automated decision making processes, which feed data into an algorithm in order to calculate a person's credit score.

Local authorities do some automated decision making, e.g. in checking eligibility for Free School Meals. HLT will address what schools need to say about this in guidance to be published regarding Privacy Notices for schools. In completing your IAR focus on what the school does. It is unlikely schools will be involved in any profiling or automated decision making processes.

Does your school use any personal data it holds for anything similar? It may simply be the case that your school does not do any profiling or automated decision making. However, it is important to identify if you do and record what personal data is subject to automated decision making and what data isn't.

3.22. **Retention**

How long will the Information Asset be kept by the school? Pupils' records should generally be kept by secondary schools at least until the pupil reaches the age of 25. For pupils with SEND records, these should be kept at least until they reach the age of 32. This will ensure schools retain records throughout the period during which any kind of legal claim can be made by a former pupil.

As part of this guidance, the Council has a Schools Retention Schedule which sets out suggested retention periods for how long various types of school record should be kept. Additionally, the Information and Records Management Society also provide a very useful retention schedule on their website (http://irms.org.uk/page/SchoolsToolkit) which contains guidance on retention of all kinds of documents in addition to those containing personal data.

3.23. **Risk / Impact**

What are the risks posed to the individual if this personal data is lost, accidentally destroyed or the subject of a data breach? What harm or distress would or could be caused? Substantial damage would be financial loss or physical harm. Substantial distress would be a level of upset, emotional or mental pain that goes beyond annoyance, irritation, strong dislike, or a feeling that the processing is morally abhorrent.

3.24. **Protective Marking**

It is recommended that schools adopt a scheme for marking documents (either paper or electronic records) to indicate their sensitivity. All personal data should be considered as sensitive and confidential.

For reference, a description of the security classifications used by the Government is available on line – go to https://www.gov.uk/government/publications/government-security-classifications

4. Application Asset Register

On the second tab of the IAR spreadsheet you will find the template Application Register. Where you have identified that Information Assets are held in software applications in your Information Asset Register, you need to clarify where the data is hosted and whether or not adequate security measures are in place. Security measures will be addressed in a GDPR compliant contract (we will provide separate guidance on due diligence re: contracts with data processors).

Advice regarding managing retention within the Capita Software will be provided prior to the scheduled software update in the autumn term. If you have any queries regarding this, please email the SIMS MIS

inbox (servicedesk@learningtrust.co.uk). If you do not use Capita SIMS, we recommend that you contact your service provider regarding this.

5. Information Audit

Once you have completed your IAR, look at each individual information asset and ask the following questions about the personal data within them;

- What is the source of the data?
- How is that data processed? What is it used for?
- Do you rely on seeking consent from data subjects and is it a genuine choice? If so, how is this consent obtained and maintained?
- Is there any onward sharing? To whom? Is there a clear legal basis?
- Who has access to the data in this information asset? Am I satisfied that only those who need to see the data can see it?
- How are people made aware of this processing activity? Should we state we are doing this in our Privacy Notice?
- Does this information asset have a clear retention period? When should it be destroyed?
- Are there adequate security measures in place to protect this data?

Once you have documented all your information assets and processing activities in your IAR, and are satisfied you have robust positive answers to the questions above, you will be able to demonstrate your compliance with the GDPR principles, thus satisfying the requirements in Article 5(2).

6. Sources of further information & advice

Sean O'Regan, HLT Freedom of Information & Data Protection Officer	Email: Sean.O'Regan@learningtrust.co.uk, Tel: 0208 820 7382
Information Commissioner's Office	https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/
Article 29 Working Party	http://ec.europa.eu/newsroom/article29/news.cfm?item_type=1358
General Data Protection Regulation	http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN
Information & Records Management Society	2016_IRMS_Toolkit_for_Schools_v5_Master.pdf (1.5 MB)