Information Asset Register

IAR

Guidance for Schools

Contents

1. Introduction

1.1 An Information Asset Register (IAR) is a simple way to help staff understand and manage the "information assets" held by you school and any **risks** associated with them. It is important to know what information is held within the school in order to protect it and exploit its potential.

1.2 The current Data Protection Act imposes responsibilities on Schools as data controllers to protect the person identifying information (PII) we process, and a data breach can result in fines up to £500,000. The General Data Protection Regulation (GDPR) is the new data protection regime the UK, effective from 25 May 2018 and whilst there are many similarities with the Data Protection Act, a big change is that the fines can be imposed where a data controller does not need to have committed a data breach, as evidence of noncompliance will suffice. Record management and retention are particularly targeted. The maximum fines are also considerably higher, up to €20 million.

1.3 Under Article 30 of the General Data Protection Regulation (GDPR) each data controller and, where applicable the controller's representative needs to maintain a record of processing activities under its responsibility. These records must be in writing or electronic form. The controller must make the record available to the Information Commissioners Office (ICO) on request. The IAR will be one method of demonstrating compliance with Article 30.

1.4 This guidance sets out a process to enable staff to understand, assess and document information assets.

1.5 This guidance will assist staff to:

- Identify their business area's information assets;
- Understand business requirements for using those information assets; and
- Document the relationships between business requirements and information assets in a way that supports schools in managing and planning its business.

2. What is an Information Asset?

2.1 An information asset is a body of information, defined and managed as a single unit so that it can be understood, shared, protected and exploited effectively. Information assets have a recognisable and manageable value, risk, content and lifecycle.

2.2 The key is to group individual pieces of information together into manageable portions (if you had to individually assess each file, database entry and piece of data you hold, you would likely have a list of millions of items and an impossible task). By grouping items at a level to match your business area's objectives, you can make this task achievable.

2.3 You might consider clusters of information which will be considered to constitute an asset. Identified information must then be documented within the IAR.

3. What is an Information Asset Register?

3.1 An IAR is an inventory or catalogue of information assets and their systems. Some examples of information assets include:

- A database of contacts is a clear example of a single information asset. Each entry in the database does not need to be treated individually; the collection of pieces of data can therefore be considered as one information asset. All the pieces of information within the asset will have similar risks associated with privacy and storage of personal information.

- All files associated with a specific project may be considered a single information asset. This might include spread-sheets, documents, images, emails to and from project staff and any other form of records. All the individual items can be gathered together and treated the same as they have similar definable content, and the same value, business risk, privacy risk and lifecycle.

- All the financial data for a business area could be considered a single asset. There are very specific risks to the school if this information is mismanaged and there may also be an obligation to provide transparency of information, which needs careful management.

4. Why Do We Need an Information Asset Register?

4.1 Information is a vital component that schools use to evidence decisions, communications, business performance, legal rights and obligations. The Register encourages greater efficiency and can be used to identify areas of potential risk, for example, the loss of personal data.

4.2 By understanding the nature of information, where it is held, how it is used, and if it is protected we can mitigate risks more easily. An IAR provides a comprehensive list of the assets that are important to the school.

5. Carrying out an Information Audit/ Building the IAR

5.1 The first step in setting up the IAR is to conduct an information audit which will assist with the identification of information assets. This need not be done from scratch as it is highly likely there will be available information about the assets that has already been collected, for example, your retention and disposal schedule and information risk register. For information on IT systems, your supplier, or IT may be able to assist.

5.2 The audit will identify:

- What information is held;
- Who holds it;
- How is it held and managed; and
- The information flow.

5.3 As a first step, consider what information is required to meet your business area's objectives. **An information asset is defined at a level of detail that allows its constituent parts to be managed usefully as a single unit.**

5.4 To perform an information audit, talk to staff from all sections of the service area to ensure all aspects of business are covered. Begin with very broad definitions and continue to split the information grouping up until it is of a suitable size.

5.5 Further guidance on how to identify "Information Assets" is set out in Appendix B.

6. Documenting Information Assets

6.1 All the information gathered about the assets which have identified, the business requirements they meet, and how they are managed must be recorded on the IAR.

6.2 The key purpose of the IAR is to document the links between a service areas information assets and its business requirements. The table attached at **Annex A** sets out what is required to complete the IAR.

6.3 One of the key fields on the IAR identifies who is responsible for making sure the asset is meeting its requirements and that risks and opportunities are monitored. This person need not be the creator of the information asset but they must have a good understanding of what the business needs from the asset are and how it needs to be capable to fulfil those requirements.

6.4 GDPR introduces a new Accountability & Governance Principle, which requires schools to maintain internal records of their processing of personal data. By formally documenting these activities and any associated risks to the asset in the IAR would be one way of demonstrating compliance with this Principle. The definition of 'Personal Data' as defined under GDPR is contained within **Annex B.**

6.5 If the data being processed is considered personal data it is important to identify and document the legal basis for processing the data in order to be lawful under the GDPR. The IAR will provide the means of documenting this to achieve compliance.

7. Maintaining and Updating the IAR

7.1 To sustain the usefulness of the IAR, it is vital to regularly maintain and update it. The Data Protection Officer will act as the owner of the register itself (but not the information assets described within it) and should follow a maintenance schedule and be reviewed at least annually.

The document should be a living document – it should be revisited as new systems are acquired, or existing systems and processes are replaced or reviewed.

ANNEX A

Instructions on Completing an Information Asset Register

1	**Data held or collected by the school**	Include a very brief description of the personal data under consideration.
2	**Data Label**	Drop-down list. Does the Asset contain personal data and or sensitive personal data? See Appendix B for definitions and examples.
3	**Information Asset Owner**	A named person who is operationally responsible for this information asset.
4	**Who has the role / access to enter information**	Note who has legitimate access to the information.
5	**Where is the data kept?**	Include a brief description of the location of the data.
6	**Purpose**	A brief note on the purpose for which the data is held.
7	**Legal basis for collection A***	What are the lawful bases for processing? The lawful bases for processing are set out in Article 6 of the GDPR. At least one of these must apply whenever you process personal data: **(a) Consent:** the individual has given clear consent for you to process their personal data for a specific purpose. **(b) Contract:** the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract. **(c) Legal obligation:** the processing is necessary for you to comply with the law (not including contractual obligations).

		(d) Vital interests: the processing is necessary to protect someone's life. **(e) Public task:** the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law. If the data is required for you to conduct the statutory duties, then select option (e).
8	**Legal basis for collection B*** **This column is only needed for items under 'Special Categories', for which it must be completed**	What is the legal basis for processing sensitive data? Meaning personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited. The lawful bases for processing are set out in Article 9 of the GDPR. At least one of these must apply whenever you process personal SENSITIVE data: **(a) Explicit Consent** - Has the subject of the data provided explicit consent to process in this context? **(b) Employment / social security / protection law** - is the data being processed for these lawful purposes? **(c) Vital interests where consent is impossible** - essentially applies in "life-or-death" scenarios - can include people affected - e.g. child protection from a data subject? **(d) Political/philosophical/religious/TU organisation aim** - applies to not-for profits - do not use.

		(e) Personal data manifestly made public by subject - where the subject has made this information public in other areas - e.g. online publishing/social media. **(f) For establishment, exercise/defence of legal claims** - where the data is processed for legal preparations. **(g) Substantial public interest** - Preventive or occupational medicine-processing is necessary for the purposes of preventive or occupational medicine. **(h) Public health in public interest -** data may be processed for the purposes of public health - Health professionals/Medicine/Social Care ONLY.
9	**If Consent selected in previous column, when is it sought?**	You must describe when consent is captured, and where it is stored.
10	**If Consent, where is record of consent stored?**	You must describe where consent records are stored.
11	**How long is data item kept / used for?**	The Department of Education has issued guidance for you. Please refer to the Department of Education Retention & Disposal (R&D) Schedule.

ANNEX B

Information Assets and Personal Data

Information Asset

An Information Asset can be defined as an identifiable collection of data stored in any manner, at any location, and recognised as having value to the EA for the purposes of performing its business functions and activities.

The following guidance will help you identify information assets within your business area:-

- The collection should be managed as a single item (e.g. All Application forms for a particular grant).
- It is not easily replaced without cost, skill, time, resources or a combination.
- You should be able to see what the risks are to holding and using the information and it should be managed proportionately to the risk(s) it represents.
- The asset is the collection of information, and not the medium in which it is stored e.g. a collection of paper files, a database, a collection of documents on a shared drive. Information technology software and hardware are not in themselves information assets, it's the information they contain which is important.
- The inputs, outputs and stakeholders should be identifiable.
- The asset may be protectively marked, but not necessarily so e.g. a spread-sheet of anonymous data may not be protectively marked, but may still be critical to the work of the business area.

So to identify your information assets, you should ask the following questions:-

- Does it have value to your business area/or the wider EA?
- How much would it cost to replace the information?
- Would there be legal, reputational or financial repercussions if it were lost?
- Would it have an effect on operational efficiency if you could not access the information easily?
- Is there a risk associated with the information?
- Is there a risk of losing the information?
- A risk that the information is not accurate?
- A risk that someone may try to tamper with it?
- A risk arising from inappropriate disclosure?
- Does the group of information have a specific content?
- Does the information have a manageable lifecycle?

Some examples of information assets, which the Senior Manager is owner of, are:-

- § A local database containing specific local information such as grant payments or budgets.
- § A collection of files e.g. associated with a specific project or programme.
- § A single casework file.
- § Local budget spread-sheets.
- § A map collection e.g. in map drawers or map cabinets.
- § Statistical information e.g. group of linked spread-sheets.
- § Research reports and associated records.
- § Information required to be maintained by law.
- § Consultation papers and all associated consultation responses.
- § Collections of information gathered from one or more external sources which may be managed or administered by The EA.
- § Sets of procedures, processes, policies.

Information Assets may be held on the intranet, on paper files, within line of business applications or shared drives. No information asset should have its only copy stored on a 'C' drive.

Further information on 'Information Assets' can be found on defining on the '**National Archives' Website**:

http://www.nationalarchives.gov.uk/documents/information_management/information-assets-factsheet.pdf

Personal Data

The GDPR applies to ‘personal data’ meaning any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier.

This definition provides for a wide range of personal identifiers to constitute personal data, including name, identification number, location data or online identifier, reflecting changes in technology and the way organisations collect information about people.

The GDPR applies to both automated personal data and to manual filing systems where personal data are accessible according to specific criteria. This could include chronologically ordered sets of manual records containing personal data.

Personal data that has been pseudonymised – eg key-coded – can fall within the scope of the GDPR depending on how difficult it is to attribute the pseudonym to a particular individual.

Sensitive Personal Data

The GDPR refers to sensitive personal data as “special categories of personal data” (Article 9), meaning data consisting of racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data, data concerning health or data concerning a natural person's sex life or sexual orientation.

Personal data relating to criminal convictions and offences are not included, but similar extra safeguards apply to its processing (Article 10).