INFORMATION ASSET REGISTER (IAR)

PREPARED BY

Michaela Bohacova
Information Compliance Officer

June 2023

Information Asset Register

An Information Asset Register (IAR) is a crucial tool for organisations to manage and document their information assets effectively. In the context of evidence item 1.1.2 in the Data Security and Privacy Toolkit (DSPT), this workbook outlines the necessary steps to create an IAR specifically tailored to meet the requirements of the item.

Overview

Under the Data Protection Act (2018) and the General Data Protection Regulation (GDPR), it is mandatory for all personal and sensitive data to have a lawful basis for both its storage and sharing.

Care providers have a legal obligation to maintain a comprehensive record of all personal data they possess for staff, residents, and families/carers, as well as the data they share with third parties.

What is an IAR?

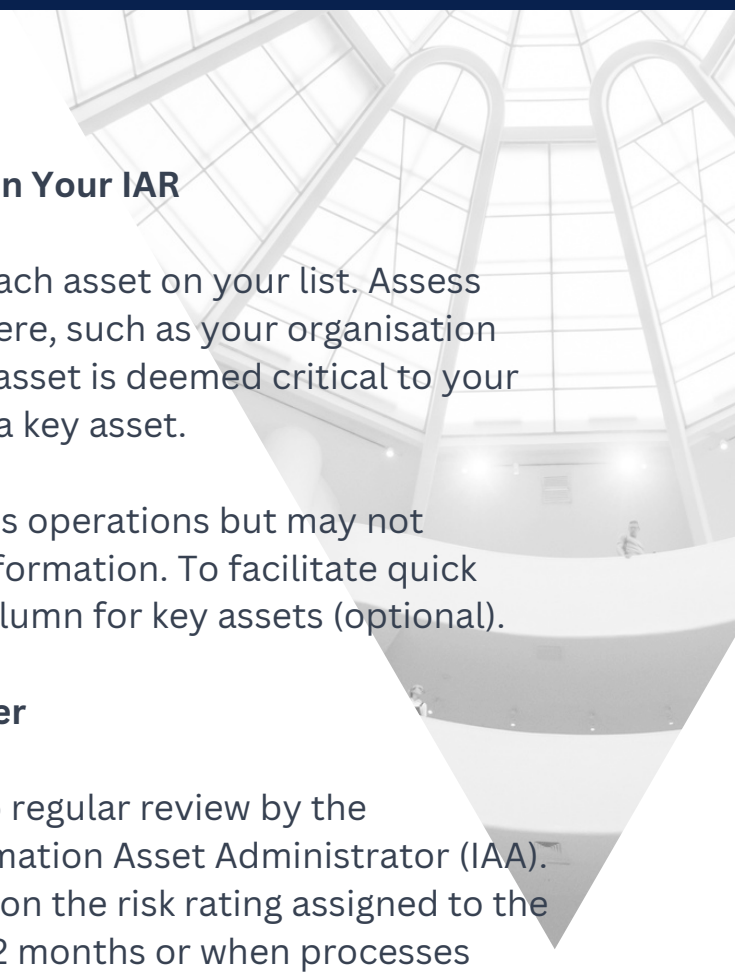
An information asset refers to valuable organisational information, such as care records in a filing cabinet, care records in planning software, and employee training records. It is crucial to consider all personal data in this regard. Recording information in various formats like paper, CD, electronic, tape, etc. is important.

It is recommended to find a balance between categories that are not too specific, like individual care plans, which could be time-consuming to document, and ensuring an appropriate level of granularity that suits your organisation.

The Value of an IAR

It serves as a crucial tool in effectively leveraging your organisation's information assets. It plays a significant role in identifying areas of duplication and promoting enhanced efficiency. Additionally, it enables the identification of potential risks, such as the loss of personal data. By gaining a comprehensive understanding of the nature of your information and its storage locations, you can effectively manage these risks with greater ease.

^1 The National Archives (2017). What is an Information Asset Register.



Identifying and Categorizing Key Assets in Your IAR

Consider the potential impact of losing each asset on your list. Assess whether the consequences would be severe, such as your organisation being unable to function without it. If an asset is deemed critical to your organisation, it should be categorized as a key asset.

Key assets are vital for your organisation's operations but may not necessarily contain the most sensitive information. To facilitate quick identification, the template includes a column for key assets (optional).

Maintaining an Information Asset Register

Information asset registers are subject to regular review by the Information Asset Owner (IAO) and Information Asset Administrator (IAA). The frequency of these reviews depends on the risk rating assigned to the asset but will occur at least once every 12 months or when processes change.

To maintain an accurate and comprehensive asset register, it is essential not to delete any information. It is crucial to maintain a complete audit trail whenever assets are relocated or modified.

If an asset is no longer in use or if the associated information flow has ceased, the following steps can be taken:

1. Highlight the corresponding row in the asset register.
2. Apply a strikethrough format to the text in the row. This can be done by pressing CTRL + Shift + F and selecting the Strikethrough option.
3. Fill in the decommissioning details in the designated green columns located on the right-hand side of each worksheet.

This function is not required for DSP Toolkit compliance but can be useful for your organisation at a local level.

^1 The National Archives (2017). What is an Information Asset Register.
^2 Information Asset Register Procedure (2021). Maintaining an Information Asset Register.

What steps should we take next?

To effectively manage personal data within your organisation, start with an information audit or data-mapping exercise. This helps clarify what data you hold and its location. Engage people from various teams to ensure comprehensive mapping of all processed data. Additionally, gaining senior management buy-in is crucial to support and resource this documentation exercise.

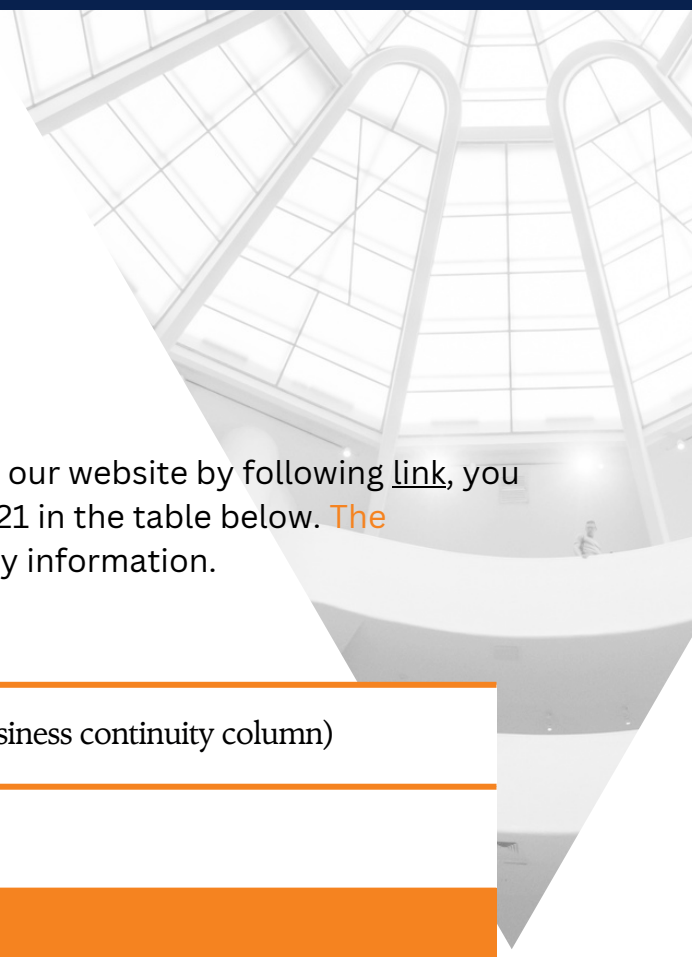
To effectively document the information required under the UK GDPR, follow these three steps after gaining an understanding of your personal data and its storage:

1. **Devise a questionnaire**: Create a questionnaire with simple, jargon-free questions to gather information from different areas of your organisation. Focus on areas that handle personal data and prompt answers relevant to documentation requirements. **Example questions:** *Why do you use personal data?; Who do you hold information about?; What information do you hold about them? Who do you share it with?; How long do you hold it for? How do you keep it safe?*
2. **Meet with key business functions:** Arrange direct meetings with departments or teams to gain a deeper understanding of their data usage. IT staff can provide insights into technical security measures, information governance staff can share retention periods, and legal/compliance staff (DPO team) can offer details on data-sharing arrangements.
3. **Review policies, procedures, contracts, and agreements:** Locate and review existing documents such as privacy policies, data protection policies, retention policies, security policies, system use procedures, data processor contracts, and data sharing agreements. Compare them with actual data processing activities to ensure alignment and capture relevant information for documentation.

Ensure your organisation's processing activities are documented in a granular and meaningful way. Account for different retention periods and the varying organisations involved in data sharing based on data categories and processing purposes. A generic list without meaningful links won't meet UK GDPR's documentation requirements.

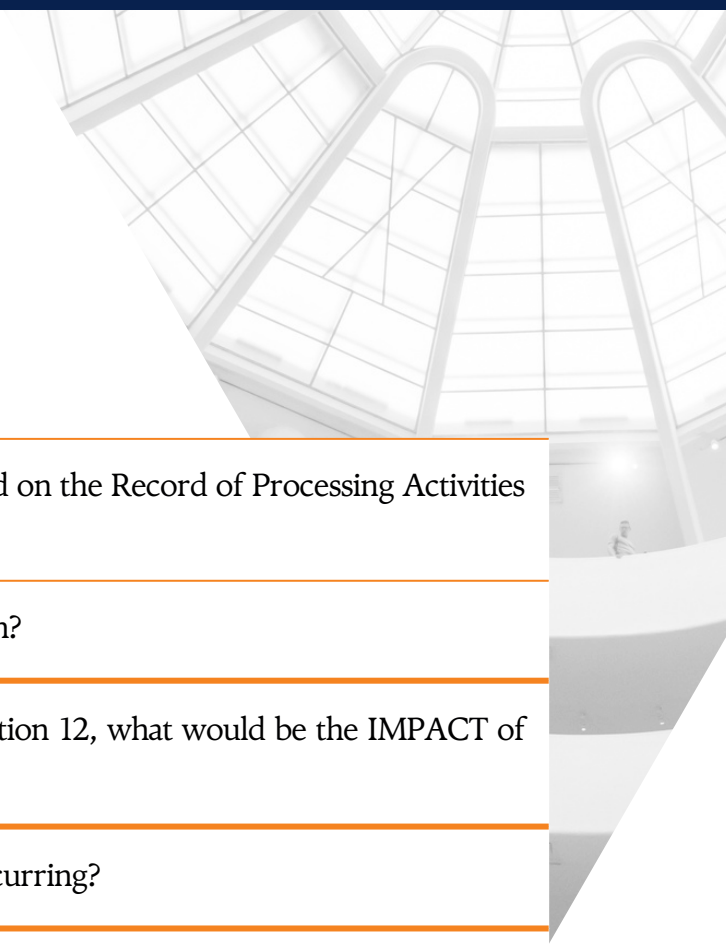
^3 ICO (2023). How do we document our processing activities?.

Template and Key Information

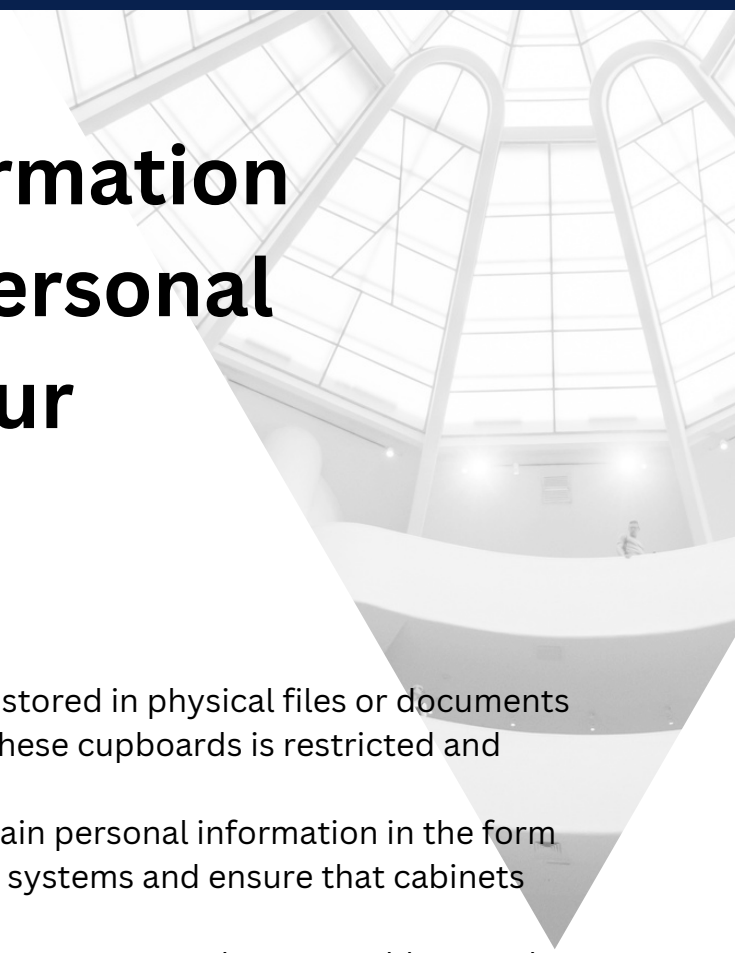


Based on the provided template, accessible via our website by following link, you must respond to each question numbered 1 to 21 in the table below. The highlighted sections in the table indicate the key information.

	Key Asset (optional, see page 1-2 guide, see business continuity column)
1.	Category of Asset
2.	Information Asset Name
3a.	Supplier Name
3b.	Contract Location
3c.	Contract Start and End Dates
4.	Date Information Asset Issued (If applicable)
5.	Date Information Asset Returned (If applicable)
6.	What Information is Kept Here and Why?
7.	Location - Where is the Information Asset?
8.	Does this contain special category data?
9.	Who is the Information Asset Owner?
10.	Is the Information Shared Externally?



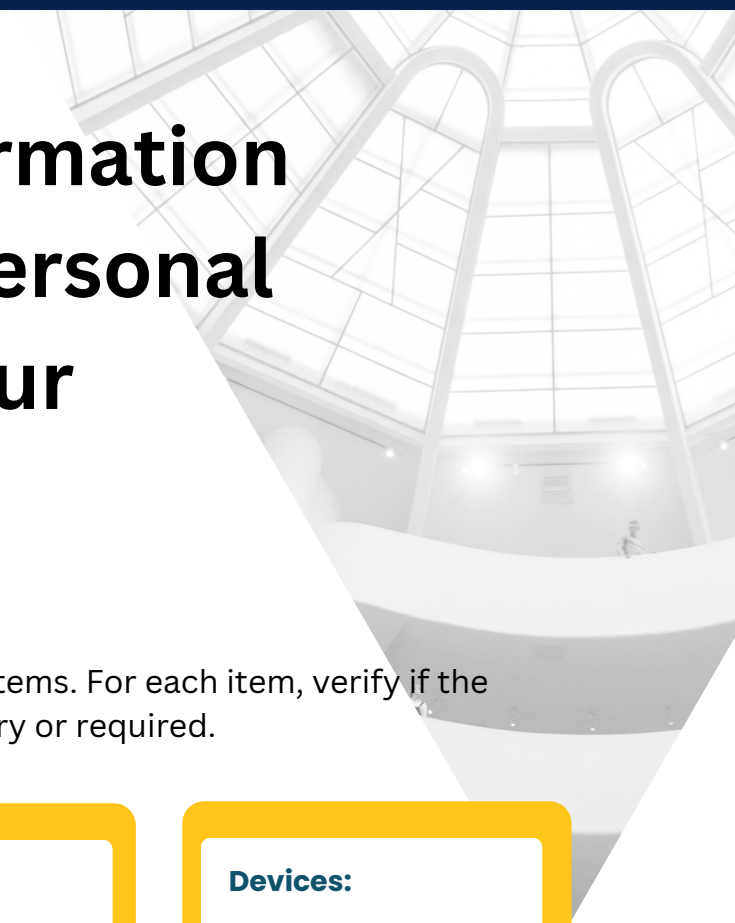
11.	[Only if Yes to 10] is the process included on the Record of Processing Activities (ROPA)?
12.	What Risks Are There if There is a Breach?
13.	Considering the risks highlighted in question 12, what would be the IMPACT of the risk occurring.
14.	What is the LIKELIHOOD of this risk occurring?
15.	Risk Score
16.	For Risks that are scored anything other than green, state and justify how you wish to either Accept or Mitigate the risk.
17.	What Risk Mitigation Actions Have Been Put in Place?
18.	Date of Last Audit.
19.	Has There Been a Breach Since the Last Audit?
20.	[Only if Yes to 19] Have All Actions Which Arose Because of the Breach been Taken?
21.	[Only if Yes to 'Key Asset'] Business Continuity Plan in place?



Examples of 'Information Assets' Holding Personal Information in Your Organisation

1. **Cupboards:** Personal information may be stored in physical files or documents within cupboards. Ensure that access to these cupboards is restricted and proper security measures are in place.
2. **Filing Cabinets:** Filing cabinets often contain personal information in the form of paper records. Implement proper filing systems and ensure that cabinets are locked when not in use.
3. **Devices:** Various electronic devices such as computers, laptops, tablets, and smartphones may hold personal information. Protect these devices with strong passwords, encryption, and security software.
4. **Posters/Lists on Wall:** Personal information may be displayed on posters or lists on the walls, such as staff contact details or patient schedules. Ensure that sensitive information is not easily visible to unauthorized individuals.
5. **CCTV Footage**: If your organization uses closed-circuit television (CCTV) systems, the recorded footage may capture personal information. Store and handle CCTV footage securely, and only retain it for the necessary period.
6. **Digital Systems:** Digital systems like NHSmail, care planning systems, eMAR (electronic medication administration record), and HR systems may contain personal information. Apply appropriate access controls, encryption, and regular data backups.
7. **Offices:** Offices may contain physical or digital records with personal information. Maintain a clean desk policy, secure physical documents, and ensure that computer screens are not visible to unauthorized individuals.
8. **Shelves:** Shelves may hold files, binders, or other physical records containing personal information. Organize and secure these items to prevent unauthorized access.

Examples of 'Information Assets' Holding Personal Information in Your Organisation



Please review the list and mark the relevant items. For each item, verify if the personal information stored there is necessary or required.

Care record filing system:

- ◯ Paper
- ◯ Computer
- ◯ Smart phone
- ◯ IPad

Posters/lists of:

- ◯ Residents' names
- ◯ Rooms numbers
- ◯ Birthdays

Devices:

- ◯ Desk top computers
- ◯ Mobile phones
- ◯ Tables
- ◯ Voicemail

- ◯ Employee finance records, pensions and bank details
- ◯ Payroll systems

- ◯ Secure Email
- ◯ NHSmail Shared mailbox

- ◯ Prescriptions
- ◯ MAR sheets
- ◯ eMAR

Lists of:

- ◯ Suppliers
- ◯ Customers

- ◯ Dietary requirements
- ◯ Allergy lists

- ◯ Employee rota
- ◯ Employee HR information

- ◯ Archived information

- ◯ NHS Community Services records

- ◯ CCTV video footage records

Key Questions in the Information Asset Register (as highlighted on page 04 and 05)

2. Information Asset Name	6. What Information is Kept Here and Why?	7. Location - Where is the Information Asset?	17. What Risk Mitigation Actions Have Been Put in Place?
Organize Information in a Centralized Location. For instance, a staff information records file could contain all personal information about employees. Take into account various formats, including paper, CDs, electronic files, tapes, USB sticks, and more.	Provide a description of the information asset type and the rationale behind its retention. **e.g.** Personal details, emergency contacts. HR files..	Document the storage location of the information asset, typically either in a secure, locked filing cabinet or within a designated folder on your computer. **e.g.** filing cabinet, the Cloud, central shared folders...	Provide an overview of the steps taken to mitigate the risk of data breaches. Keep the description concise without going into excessive detail.

- Use the table below to list each information asset and its contents.
- Repeat the four steps until all information assets are listed,
- Conduct a thorough inspection of the building and offices to ensure all information assets are accounted for.
- Utilize the checklist of examples of 'information assets' on page 7 to ensure all personal information is appropriately assigned to an asset.
- Perform a final review of all supplier contracts to determine if any personal information is stored by them.

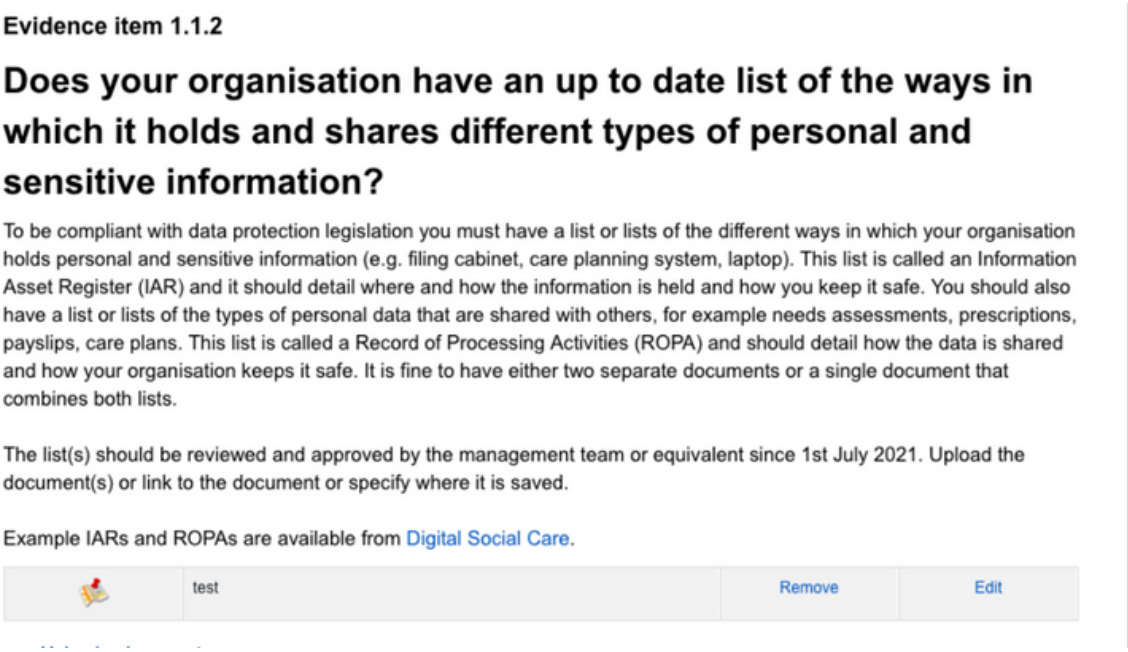
Information Assets Records Key Questions			
2. Information Asset Name	6. What Information is Kept Here and Why?	7. Location - Where is the Information Asset?	17. What Risk Mitigation Actions Have Been Put in Place?

What are the Final Steps to Take...

Once you have completed the table, the final steps are as follows:

- Insert the key information into the template.
- After completing the above step, you are ready to proceed with filling out the rest of the template.
- Review the IAR and obtain approval
- Complete the evidence item 1.1.2 with both ROPA and IAR in your DSPT

Did you know that completing both the IAR and ROPA documents for your practice ensures compliance with data protection legislation? Once these documents are in place, you can confidently tick and complete question 1.1.2 on the Data Security and Protection Toolkit (DSPT).



Evidence item 1.1.2

Does your organisation have an up to date list of the ways in which it holds and shares different types of personal and sensitive information?

To be compliant with data protection legislation you must have a list or lists of the different ways in which your organisation holds personal and sensitive information (e.g. filing cabinet, care planning system, laptop). This list is called an Information Asset Register (IAR) and it should detail where and how the information is held and how you keep it safe. You should also have a list or lists of the types of personal data that are shared with others, for example needs assessments, prescriptions, payslips, care plans. This list is called a Record of Processing Activities (ROPA) and should detail how the data is shared and how your organisation keeps it safe. It is fine to have either two separate documents or a single document that combines both lists.

The list(s) should be reviewed and approved by the management team or equivalent since 1st July 2021. Upload the document(s) or link to the document or specify where it is saved.

Example IARs and ROPAs are available from Digital Social Care.

	test	Remove	Edit

SEND US YOUR ROPA OR IAR, AND WE WILL BE HAPPY TO REVIEW IT FOR YOU.

FEEL FREE TO GET IN TOUCH WITH OUR DATA PROTECTION OFFICER, LIBERTY APTED, AT **LIBERTY@LMCUKSERVICES.CO.UK** OR CALL **0117 387 8972**.