Corestream Information Asset Manager Quick Reference Guide

&

Information Asset Owner Guidance

Contents

1. Introduction

The General Data Protection Regulation (GDPR) introduced in 2018 created new obligations on the University to record the types of information it holds, along with other details about that information including where it is located, who has access to it and whether it contains personal data. Information held is an ‘asset’ as it is of value to the University. Where information is held, it must be recorded on a central register.

The University has adopted the Corestream Information Asset Manager (IAM) as its central register of information assets.

Each Division/Faculty/School is responsible for recording their assets on the central register, reviewing them annually as well as updating assets as and when the asset changes. This is an essential requirement in order to demonstrate compliance with GDPR.

Failure for the University to record and monitor its information assets may lead to fines of up to 4% of the University’s budget; in 2017/18 this would have meant a fine of up to £17m.

1.1 What is an information asset?

An information asset is a body of information, defined and managed as a single unit so it can be understood, protected, shared and exploited efficiently. Information assets have recognisable value.

Examples of information assets include:

- A database of contacts
- All files associated with a specific project
- Staff sickness records
- Meeting or Board papers
- Exam scripts

1.2 How do I access IAM?

The system is accessible via any desktop or tablet browser by using the link provided. Two authentication methods are available – either Multi-Factor Authentication (MFA) using your usual University username and password or Single Sign On (SSO) where it is available.

1.3 What are the different roles within IAM?

Role	Overview	How role is decided?
Information Asset Owner (IAO)	The IAO is responsible for their assets but not required to administer the IAM e.g. by approving assets. They will however be able to view the content.	University Hierarchy
Administrator	Responsible for administering assets, making changes and completing review tasks. The Administrator can only edit and review assets that they are named on (via the My Register pages).	Nominated by Head of Faculty/Division or IAO

1.4 What are the different menus within IAM?

IAM is broken down into the following navigation items and access to each area is governed by permission groups on the system. The main areas are:

Area	Contents
My Registers	This will show you Information Assets, Risks and Actions relating to yourself
All Registers	This will show you Information Assets, Risks and Actions relating to all users
Data Role Declarations	The University is not using this feature yet
Breach Reports	The University is not using this feature yet

Reports	A full suite of reports showing data related to the system
Guidance	Provides guidance notes and a quick reference guide to key features of the system
Administration	Used by information governance staff to set up and maintain the platform

2. Identifying an Asset

Having read this far, you will already likely have identified several assets relevant to you. Examples might include:

- An Excel spreadsheet of commercial contacts for student placements on the shared network drive
- Agendas for your Divisional meetings kept within SharePoint
- Paper files kept within a filing cabinet in an office
- Draft copies of policies and procedures kept on the shared network drive
- Bespoke systems used by your Division/Faculty/School e.g. *Symphony* for Catering Services or *Qwickly* used by Visa Services
- An Excel spreadsheet containing a list of student representatives contained on the shared network drive
- Copies of letters sent to students kept on the shared network drive

3. Logging an Asset

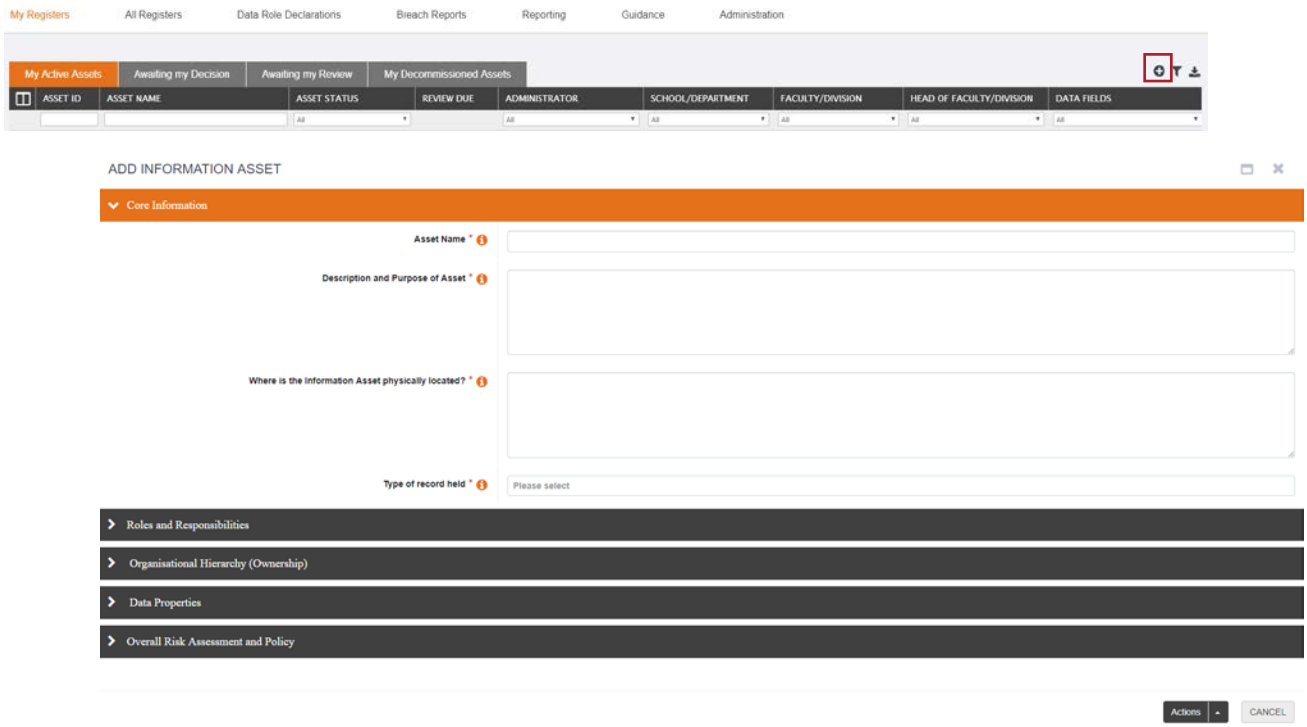
3.1 Core Information

Once you have identified an asset that you are responsible for, it's time to log it within IAM. This is a straightforward task and is completed by using drop boxes, tick boxes and a small number of free text boxes. *Use the pop-up boxes to help you complete the fields (click on).*

When registered, you will be sent an email with a link to IAM, no password is required as the system runs from your UoB password.

3.1.1 Select *My Asset Register*

3.1.2 Select  from the three icons on the right of the screen. This will open up the asset submission form.



3.1.3 Your Asset Name should be a high-level identifier for your asset. You should avoid names like ‘Amy’s Spreadsheet’ and should instead give some indication of what the asset contains. Good examples include:

- Agendas, minutes and supporting papers for key meetings
- Hourly paid tutor contract spreadsheet
- Unit and programme approval documentation
- Lecture slides, notes and handouts

- H&S risk assessments
- Letters to students

3.1.4 The Description and Purpose of Asset should give a reviewer some idea of what you use the asset for in your area. For example, if your Asset Name was '*External examiner appointment',* a good Description and Purpose would be '*records maintained in relation to appointing external examiners. Retained in case of query/dispute'.*

3.1.5 Where is the Information Asset physically located will generally be a straightforward question. If the asset is located on the shared network drive then you would be expected to copy and paste the full file path into the field. If the asset is kept in a filing cabinet then we would expect the address and room number (or approximate) of where that physical asset was located. If the asset is a piece of software such as a system like *F2,* we would expect an administrator to know whether the system is hosted on University servers or in 'the cloud'.

We ask for such detail in relation to where an asset is physically located as it allows the University to manage risk and demonstrate to an auditor that appropriate security measures are in place. There have been a number of instances, in particular within the health sector, where an organisation has decommissioned part of its estate and left behind sensitive information. This carries a significant financial penalty.

The GDPR has also added emphasis on understanding whether data controlled by the University is shared outside of the European Economic Area e.g. to the United States or Norway. Where this is the case, the University is required to put extra safeguards in place.

3.1.6 The Type of Record Held may often be mixed, however we would encourage you to use whatever appears most reasonable to you and select more than one if held physically and electronically.

Examples

- *SITS* would be a structured database, as would *F2*, *Qwickly* or *MyERP*
- A hard copy personnel file contained within an archive would be a physical asset, as would printed copies of policies or procedures kept within a filing cabinet
- An Excel spreadsheet stored on the H:\ drive would be an electronic asset as would any emails you have saved to your H:\ drive, OneDrive or SharePoint

3.2 Roles and Responsibilities

3.2.1 The Information Asset Owner (IAO) is the most senior person who understands what the information is, where it is held, what it is used for and who has access to it. The IAO is the job title of the person responsible for the asset and not the name of the person themselves. For example, the IAO of the *Summer Lets Database* will be the Head of Accommodation Services. Likewise, the IAO for the *Exam Incident Report Forms* asset will be the Examinations, Timetabling and Graduation Manager.

3.2.2 The Administrator/Other Administrators will be the staff responsible for managing the asset within IAM. They may in theory never use the asset they are logging, however they should be aware of the same things as the IAO in 4.1. The Administrator/Other Administrator can only be a member of staff who has been set up within the system. To add new Administrators to the list, you will need to contact data-protection@bristol.ac.uk.

3.2.3 'Who can access the data' is a key question under GDPR. We all want our privacy and the best way the University can achieve this is by limiting the number of people who can access data; data, especially that which is personal, must not be accessed by an individual who does not have a business need for accessing that data.

In this field you should record the job titles of those with access to the information. Where information is freely accessible to a large number of staff, then it will be acceptable to record this in a way such as *'all Faculty staff and staff from Change Management'.* This will be especially important if you know you are moving to SharePoint in the near future.

3.2.4 Whether or not data is shared with a third party may often create difficulty for staff in completing this section. A third party is any party outside of the University. Very often it will be the case that you don't routinely share data, however that data would likely be shared if there was a request. Where this is the case, the data shall be considered as not shared with a third party. If circumstances change and you start routinely sharing data with a third party, then you should update your asset on IAM.

Where data is always shared with a third party as a matter of routine, that organisation you share with should be recorded in the '*Who can access the data?'* field.

3.3 Organisational Hierarchy (Ownership)

3.3.1 Within IAM, there are two distinct categories of asset. One belonging to the academic structure and one belonging to Professional Services. You will likely know which structure you sit within and this should be selected in Organisation Level 1.

3.3.2 Likewise, you should know your own Faculty/Division and School/Department therefore this can be populated with ease.

3.3.3 The Head of Faculty/Division field will populate itself based on the structure managed by the information governance team. Where this is incorrect, you should inform data-protection@bristol.ac.uk.

3.3.4 The University is not currently using Organisation Administrators or Organisation Viewers in all instances so this will likely be greyed out.

3.4 Data Properties

3.4.1 The 'Data Properties' section requires the Administrator to have a good knowledge of the asset and the confidence to identify personal data. If you are not the IAO then you should check the information in this section with them.

3.4.2 How often a record is accessed will be a question of judgement for the Administrator. For example, for the purposes of recording an asset, a personnel file stored in a third-party records storage provider will 'never' be accessed. This isn't to say that it won't ever be accessed, just that the chance is so remote and certainly less than 'rarely'. A record accessed 'rarely' may be physical documents within a filing system in an office. Largely, these are reference documents that may have now been replaced by digital documents.

3.4.3 The quantity of records is just a realistic estimate. There is no expectation on an Administrator to manually count each record, especially where that record is physical. The number of records within a folder on a computer can be determined by right clicking the folder and selecting properties. The information box will tell you how many records it contains e.g. '42 Files, 16 Folders'.

3.4.4 The GDPR only concerns personal data and is largely uninterested with any other sort. Personal data is any data that relates to a living person. Examples of personal data include, but are not limited to:

Field	Example	Field	Example
FName	Jane	SName	Doe
DOB	01/01/1970	Address	1 High Street, Bristol
Post Code	BS2 8DZ	Phone No	01275 000 111
Email	Joe.Bloggs@email.com	Driving Licence No	DOEJA657054SM9FG
Passport	925665416	IP Address	37.187.129.177
Gender	Female	IMEI	354518589544
Photo	JaneDoe.png	CV	JaneDoeCV.pdf
VRN	CE68LMG	Interview Notes	JaneDoeFeeback.docx

NI No	PQ 12 34 56 A	DNA	JD010111970.genome
Salary	£44,250	MAC Address	00:30:6E:FSE0:7D

If the asset you are recording contains any of these, then it will be considered personal data.

3.4.5 The data groups should be self-evident to you. Where there are many data groups, you should pick the one that is most numerous.

3.4.6 The GDPR Data Classification (which uses the University's Information Classification Scheme) is again an area where you will have to exercise discretion. An understanding of the asset you are recording will be imperative here:

- Public – May be viewed by anyone, inside or outside the organisation
- Open – Available to people who are at the University in any of these groups: staff, postgraduate researchers, and taught students. This is not the same thing as 'everyone at the University'.
- Confidential – Access is controlled and restricted to a limited group of people
- Confidential and Sensitive – Access is restricted to a small number of people who are listed by name.
- Secret – Known only to a very small number of University staff and postgraduate researchers who have been vetted and cleared for access.

3.4.7 A key tenet of GDPR is that data can only be retained for as long as necessary. There are very few types of personal data that can be retained indefinitely. When determining whether you apply a retention period to your data, you should look realistically at whether the data needs to be retained at all. Refer to the University's Records Retention Schedule for more guidance. We urge you to use this as an opportunity to consider disposing of records.

3.5 Overall Risk Assessment and Policy

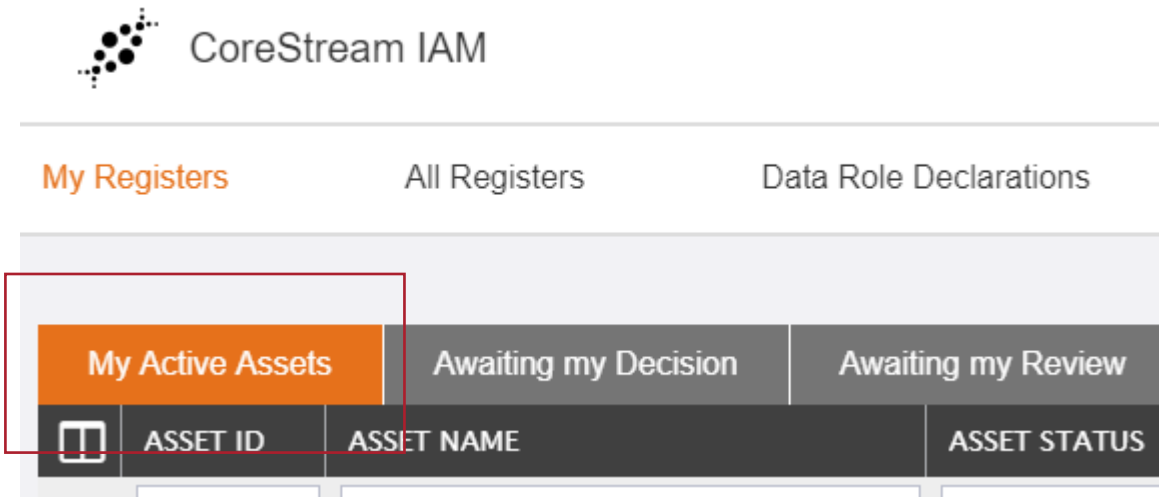
3.5.1 A Major Asset is one which you cannot function without. Telephony and email are examples of University information assets that would cause significant disruption.

3.6 Completion

3.6.1 When you've completed the form you should submit your asset for review to the information governance team. This will be reviewed and will either be approved or returned to you with recommendations for changes e.g. apply a retention limit. The team will not return minor issues so you should not be concerned about submitting a significant quantity of assets.

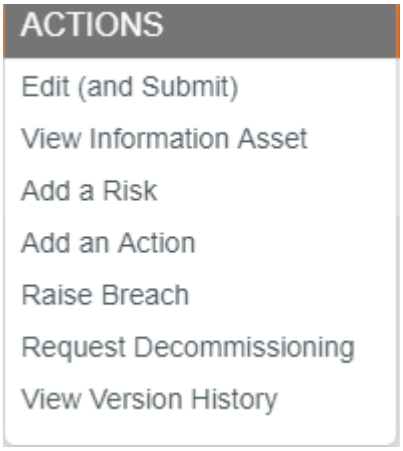
4. Searching and Editing a Submitted/Approved Asset

4.1 If you submit an asset for review and realise you have made a mistake you will need to search for that asset and update the fields. Clicking My Active Assets will return a list of all assets that you have submitted, regardless of whether they have been approved or not.



4.2 Find your asset in the list:

Clicking anywhere on the asset will bring up an actions menu. Here you can view or edit that asset.



4.3 Clicking *Edit (and Submit)* will bring you to the same form as detailed in [2].

5. Reviewing Your Assets

5.1 Once a year, you will receive an automated email from the IAM asking you to review the assets for which you are responsible as the Administrator. Click on an asset in the 'My Active Assets' tab and select 'Review Asset' (**not Edit and Submit**) to review the asset record and check the information is still accurate. If you make any changes, please add a note of these in the comments box at the top. You can now submit for review.

6. Decommissioning an Asset

6.1 At any point in the review cycle, you may decommission an asset. Decommissioning is a record of destruction and removes the asset from the list of the University's active assets. Decommissioning is especially important when you are removing sensitive data e.g. medical records, human resources records etc.

6.2 Decommissioning should not be used where only part of the information asset is being destroyed. Where this is the case, the Administrator should update the volume of records and leave a comment in the Comments field at the top of the submission form notifying the reviewer that several records that were once within this asset have now been destroyed.

6.3 Decommissioning is a simple process that can be achieved by looking at My Active Assets and clicking anywhere on the same line as the asset.

6.4 Click, Request Decommissioning. This will bring you to the familiar asset submission form as seen throughout this process. If the number of records you are destroying remains the same, then you can continue down to:

6.5 Decommissioning is not automatic and will send a review notification to the information governance team. **You should continue to destroy the asset and need not wait until the decommissioning is confirmed.**

7. Further Guidance for Information Asset Owners

7.1 Introduction

Every process in the University is dependent on the collection and management of information. Information supports research, teaching, funding applications, student administration, staff administration, engagement with customers and businesses and compliance with the requirements of bodies such as the Higher Education Statistics Agency, the funding councils, law enforcement and other bodies. The management

of information is paramount to the successful and continued operation of the institution.

Information legislation provides key frameworks and boundaries for our actions in respect of the University's information resources. Understanding what is required for the protection of information and the circumstances in which information may be requested, disclosed or withheld, informs processes and procedures and ensures the University and its staff do not take actions which could attract significant financial or reputational penalties. Understanding the appropriate way to mitigate problems should they arise helps to minimise the potential for harm to the University, its students, stakeholders and other partners. Such awareness is fundamental to the successful operation of a modern organisation.

7.2 Information Governance Framework

The IAO role sits within the framework of responsibility and accountability for the effective, efficient, safe and compliant management of the University's information assets.

The framework aims to ensure that each information asset has a clearly defined administrator/manager who is responsible for that asset on a day to day basis. The manager implements the Information Governance policies and procedures and instructions to manage that asset and provides regular (and exceptional) reports to the IAO for that asset who is responsible and accountable for ensuring that information assets within their area are managed compliantly. The IAO in turn provides compliance reports (regular and exceptional) to the Information Governance Manager who in turn reports to the Senior Information Risk Owner (SIRO).

7.3 IAO Role and Responsibilities

IAO's must be senior/responsible individuals involved in the relevant business units. Their role is to understand what information is held, what is added and what is removed, how information is moved, who has access to it and why. As a result they are able to understand and address risks to the information and ensure that information is fully used within the law for public good. They may be called upon to provide written judgement of the security and use of their asset annually to support the audit process.

Information Asset Owners are directly accountable to the Senior Information Risk Owner (SIRO) and must provide assurance through the Information Governance Manager that risk is being managed effectively and in respect of the assets that they 'own'.

It is important to distinguish IAO's from those staff who have been assigned responsibility for day to day management of information risk on behalf of the IAOs, but are not directly accountable to the SIRO.

The SIRO/IAO hierarchy identifies accountability and authority to effect change where required to mitigate risks.

IAOs are responsible for:

- Leading and fostering a culture that values, protects and uses information for the success of the organisation and benefit of its customers;
- Knowing what information comprises or is associated with the asset and understands the nature and justification of information flows to and from the asset;
- Knowing who has access to the asset and why, whether it be system or information to ensure access is monitored and compliant with policy; and
- Understanding and addressing risks to the asset and providing assurance to the SIRO via the Information Governance Manager

The University needs to ensure that its IAO's possess the necessary support, knowledge and skills to undertake their role effectively and to provide periodic statements of information assurance to the SIRO via the Information Governance Manager. The IAO should refresh their knowledge of information risk at least annually.

Leads and fosters a culture that values, protects and uses information for the success of the organisation and benefit of its customers

- To understand the University's Information Governance policies and monitor their compliance;
- To take visible steps to support and participate in that plan (including refreshing one's own knowledge);
- To ensure that staff understand the importance of effective information governance and receive appropriate education and training; and
- To consider whether better use of any information held is possible, within applicable information governance rules, or where information is no longer required.

Knows what information the asset holds, what enters and leaves it and why

- To maintain an understanding of 'owned' assets and how they are used;
- To approve and minimise information transfers while achieving business purposes;
- To approve arrangements where it is necessary for information to be put onto portable or removable media like laptops, tablets/phones and USB drives and ensure information is effectively protected to information governance standards; and
- To approve the information disposal mechanisms for the asset.

Knows who has access and why, and ensures their use is monitored and compliant with policy

- To understand the University's policies on the use of information and the management of information risk;
- To ensure decisions on access to information assets are taken in accordance with the information governance policy and best practice;
- To ensure that access provided to an asset is the minimum necessary to satisfy business objectives;
- To ensure that the use of the asset is checked regularly and that use remains in line with the policy.

Understands and addresses risk to the asset and provides assurance to the SIRO via the Information Governance Manager

- To seek advice from the Information Governance Team subject matter experts when reviewing information risk;
- To conduct Data Protection Impact Assessments for all new projects;
- To undertake regular risk assessment reviews for all 'owned' information assets in accordance with guidance and report to the SIRO, ensuring that information risks are identified, documented and addressed
- To escalate risks to the SIRO via the Information Governance Manager where appropriate and to make the case where necessary for new investment to secure 'owned' assets; and
- Provide assurance when required to support annual audit processes.

7.4 Training

The IAO will be required to familiarise themselves with this document and the associated suite of Information Governance policies, as well as ensure that they (along with all other staff who come into contact with their information assets) have completed the University's mandatory training modules hosted in MyReview.

7.5 Resources

- University of Bristol Information Governance webpage
    - Data Protection Officer – data-protection@bristol.ac.uk
- Information Security
    - Information Security Manager – cert@bristol.ac.uk
- Information Commissioner's Office
- Gov.uk Cyber Security for Business