Create data request

- Privacy officer role |]
- Data requests |]
- Responding to data requests |]
- Automatic approval of data export and deletion requests |]
- Deletion of user data |]
- Allowing only the privacy officer to download data |]
- Data registry |]
  - Example categories |]
  - Data registry set-up |]
  - Setting categories and purposes for existing contexts |]
- Data deletion |]
- Capabilities |]
- Plugin privacy registry |]

The **Data privacy** functionality provides the workflow for users to submit a data request (also known as a subject access request or SAR) and for the site administrator or privacy officer to process these requests.

- 1 Privacy officer role
- 2 Data requests
- 3 Responding to data requests
- 4 Automatic approval of data export and deletion requests
- 5 Deletion of user data
- 6 Allowing only the privacy officer to download data

- 7 Data registry
  - 7.1 Example categories
  - 7.2 Data registry set-up
  - 7.3 Setting categories and purposes for existing contexts
- 8 Data deletion
- 9 Capabilities
- 10 Plugin privacy registry

Privacy officer role |]

It is recommended that you create a Privacy officer role and assign it to the person responsible. If there is nobody on the site with the role of privacy officer i.e. nobody with the capability to manage data requests, then a site admin can respond to data requests and manage the data registry.

Data requests |]

300px-requesting_data.png
Requesting data

Any user can send a message to the privacy officer via the 'Contact the privacy officer' link on their profile page.

In addition, they can request a copy of all of their personal data or request that their personal data should be deleted as follows:

1. Go to your profile page (via the user menu).
2. Click the link 'Data requests' then click the 'New request' button.
3. Select 'Export all of my personal data' or 'Delete all of my personal data' as appropriate.
4. Save changes.

300px-Request_approved.png
Request approved

The privacy officer will then receive a data request notification.

If the user has requested a copy of all of their personal data, once the request is approved, they will receive a notification to inform them that their personal data may be downloaded from their Data requests page. The user has by default one week to download their data before the download link expires. (An administrator can set a different expiry time for the data request in 'Privacy settings' in the Site administration.)

Note: Users on Windows computers are advised to use a program such as 7zip to extract their data from the downloaded folder, as the standard Windows unzipping feature will display an error message.

If the user has requested that their personal data should be deleted, once the request is approved, they will receive an email to inform them and they will no longer be able to log in to the site.

Responding to data requests |]

300px-viewing_a_data_request.png
Viewing a data request

The privacy officer can respond to data requests as follows:

1. Go to 'Data requests' in the Site administration (or follow the link in the data request notification).
2. In the Actions dropdown, select View, Approve, or Deny as appropriate.

If the user has sent a message, the privacy officer can view the message and copy the user's email address, then reply via email. In Moodle 3.5.2 onwards, after replying they can mark it as complete.

Automatic approval of data export and deletion requests |]

Data export and deletion requests may be automatically approved, rather than the privacy officer having to manually approve each one. This feature may be enabled in Site administration / Users / Privacy and policies / Privacy settings.

Deletion of user data |]

See the ongoing tracker issue MDL-62843 Moodle is not clear on data retention when deleting a user.

What data is deleted and the behaviour within individual activities varies based on the activity itself. Taking Assignment and Forum as examples.

For Assignment the submissions for the deleted user are also removed, however, any files related to those submissions are NOT deleted, they still exist on the file system, and they still appear in Report Builder reports. But there is no way to access or remove them.

For the Forum activity the posts are removed with a comment that the content is no longer available. The user's name is replaced by Deleted user.

Allowing only the privacy officer to download data |]

In Moodle 3.5.2 onwards, organisations with multiple systems and a centralised request process can prevent users from downloading their own data and instead enable a privacy officer to download it for them.

1. Go to 'Define roles' in the Site administration.
2. For the authenticated user role unset the capability Download your own exported data and save changes.
3. For the privacy officer role allow the capability Download exported data for everyone and save changes.

The privacy officer can then make a data request on behalf of a user (via 'Data requests' in the Site administration), approve it and later download it via the Actions dropdown menu. In this situation, the privacy officer will receive notification messages and NOT the user.

Data registry |]

300px-data_registry.png
Data registry

The privacy officer can set purposes (why the organisation is processing data) with retention periods and categories for data stored in Moodle in the data registry. Different types of data may need to be stored for different lengths of time. For example, student submissions to an assessment may need to be retained indefinitely to be able to provide evidence of student accomplishments, whereas general coursework such as forum posts might only be retained until graduation + 12 months.

A default purpose and retention period may be set for course categories, courses, activity modules and blocks. The retention period is measured from the course end date for the course that an activity is in. For a user it is from the last login time for any user who is no longer enrolled (or has

already been deleted).

Example categories |]

- Administrative: Civil status, identity, identification data, images ...
- Personal life (lifestyle, family situation, etc.)
- Economic and financial information (income, financial situation, tax situation, etc.)
- Connection data (IP address, logs, etc.)
- Educational Data (Assessed Coursework, exam scripts etc.)
- Records of Education Attainment (Results of exams, assessments, qualifications awarded etc.)
- Location data (travel, GPS data, GSM, etc.)

Data registry set-up |]

To add purposes and categories:

1. Go to 'Data registry' in the Site administration.
2. In the Edit menu select Categories.
3. On the 'Edit categories' page, click the + button to add a new category.
4. Enter a category name and description then click the Save button.
5. Go to 'Data registry' again and in the Edit menu select Purposes.
6. On the 'Edit purposes' page, click the + button to add a new purpose.
7. Enter a purpose name, description and retention period then click the Save button.

Purposes and categories need to be created before they can be set as defaults. Note that default data registry categories and purposes are only applied to all newly created instances of that type (a course for example). Any content that has been created before defaults are set are not impacted.

To set default categories and purposes:

1. In 'Data registry' in the Site administration click the 'Set defaults' button.
2. Select a default category and purpose for the site, and for users, course categories, courses, activity modules and blocks as required.
3. Save changes.

Setting categories and purposes for existing contexts |]

The Data registry interface is used for navigation the contexts of the site to set the category and purpose for them, and thus the data retention period for that context.

At the very least, the site admin should set the category and purpose at the site level. Once this is saved, all lower contexts will inherit from that level. The admin can then choose to set different category and purposes for different levels of context, such as having a specific course with a longer or shorter retention period thus overriding the inherited values.

Data deletion |]

The Data deletion page (Site administration / Users / Privacy and policies / Data deletion) lists the contexts that are past their allocated retention period and need to be confirmed for user data deletion. Once the selected contexts have been confirmed for deletion, the user data related to these contexts will be deleted on the next execution of the "Delete expired contexts" scheduled task.

Capabilities |]

- Manage data registry
- Manage data requests
- Make data requests for children
- Download exported data for everyone
- Download your own exported data
- Request data deletion for minors
- Request data deletion for yourself
- Request data deletion on behalf of another user

Plugin privacy registry |]

The Plugin privacy registry (Site administration / Users / Privacy and policies / Plugin privacy registry) lists all plugins in Moodle, and identifies whether they comply with the privacy API or not. Any plugins which are flagged with the warning icon do not yet implement the Moodle privacy API. If this plugin stores any personal data it will not be able to be exported or deleted through Moodle's privacy system.

Source: docs.moodle.org/503/en/Create data request — MoodleDocs (GPL) · Imported 2026-11-10.

□□□ #1

□ cocobook-sync □□□ 2026-11-10 12:49:20 UTC

□ cocobook-sync □□□ 2026-11-10 12:49:21 UTC