



---

## TRIM: Applying Access Controls to Documents

---

University Documents (excluding document types listed at the end of this guideline) automatically take the access restrictions of the file to which they are saved. However, there may be some documents that need different access from their file.

You are able to apply Access Control to a Document at various stages as follows:

- While completing the Document registration on the Record Entry Form through the Access Tab,
- After the Document has been registered by either:
  - highlighting a Record (Document) from a search results screen and clicking on the right mouse button and selecting Properties and then selecting the Access Tab; or
  - highlighting a Record (Document) from a search results screen and clicking on the right mouse button and selecting Audit/Security - Security/Access.

The following example shows how to restrict access to your own business unit and RAMS staff.

<p>Search for the document</p> <p>Highlight the document in the search results</p> <p>Right-click &amp; select: <b>Properties</b></p>	<p>The screenshot shows a web-based search interface. On the left, there are navigation options: 'Favourites', 'Records', 'Schedules', and 'Saved Searches'. The main area displays a list of records with columns for 'Record Number' and 'Title'. The record with ID 'D11/623066' is selected. A right-click context menu is open over this record, showing options like 'Tag All', 'Untag All', 'Copy', 'View', 'Edit', 'Check Out', 'Check In', 'Supercopy', 'Details', 'Locations', 'Workflow', 'Communications', 'Electronic', 'Administrative Tools', 'Send To', 'Remove From', and 'Properties' (which is highlighted). Below the list, a detailed view of the selected record is visible, showing its title 'TRIM Advanced Training - Manual (For P...', date created 'Wednesday, 30 November 2011 at 11:28 AM', date registered 'Thursday, 1 December 2011 at 1:26 PM', and file number '05/007507: STAFF DEVELOPMENT - TRA...'. The 'Properties' option in the context menu is highlighted with a blue bar and the keyboard shortcut 'Alt+Enter'.</p>
---	--

Select the tab:  
**Update Security and Access Policy**

Leave the *Security Level* set to:  
**Unclassified**

Leave the *Active Caveats* field blank

[Advice on the use of *Caveats* can be sought from RAMS]

Access To	Details
<input checked="" type="checkbox"/> View Document	Based on Container 05/007507: People in (Records & Archives Manage
<input type="checkbox"/> View Metadata	Based on Container 05/007507: People in (Records & Archives Manage
<input type="checkbox"/> Update Document	Based on Container 05/007507: People in (Records & Archives Manage
<input type="checkbox"/> Update Record Metadata	Based on Container 05/007507: People in (Records & Archives Manage
<input type="checkbox"/> Modify Record Access	Based on Container 05/007507: People in (Records & Archives Manage
<input type="checkbox"/> Destroy Record	Based on Container 05/007507: People in (Records & Archives Manage
<input type="checkbox"/> Contribute Contents	Based on Container 05/007507: People in (Records & Archives Manage

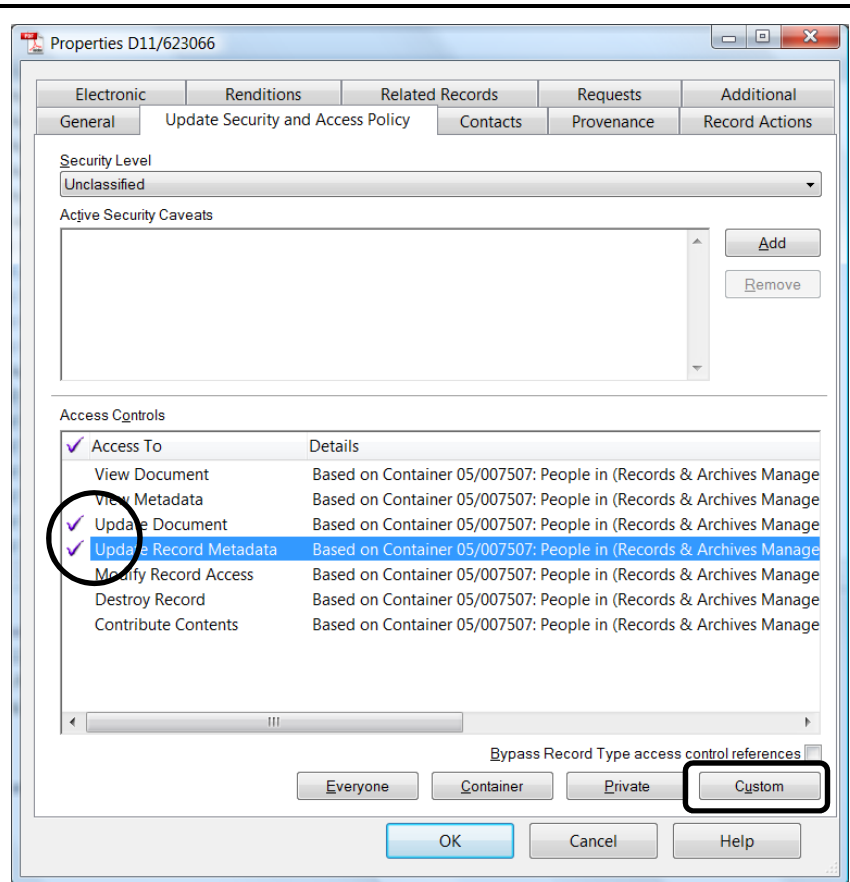
Select the Access Controls tasks that you wish to modify by tagging them.

You can do this by clicking your left mouse button in the area to the left of each item.

In this example we have chosen:

- Update Document &
- Update Record Metadata

Click:  
Custom



### Access Control Options Available

You may modify Access Control for the following tasks:

- **View Document** – allows a person to see the attached electronic document
- **View Metadata** – allows a person to see the record's registered information (*that is, information about the record*)
- **Update Document** – allows the Check In and Check Out of attached electronic documents for modification
- **Update Record Metadata** – allows record information to be modified
- **Modify Record Access** – allows modification of Security and Access Controls for the selected record
- **Destroy Record** – the Destroy Record option is only available to RAMS staff.
- **Contribute Contents** – allows staff to contribute contents even if they cannot see the file (relevant for files only, not relevant for documents).

Once you have selected the tasks you wish to restrict, you have the following options for Access Controls:

- **Everyone** – DO NOT USE THIS SETTING. This will provide access to all staff at UWS.
- **Container** – The document will inherit the Access Control properties of the file it is enclosed in. This is particularly useful for workgroups who only have access to a project folder.
- **Private** – DO NOT USE THIS SETTING. This will provide access only to the currently logged on user. When you click Private, your user name will be placed in the Details field.
- **Custom** – Specify persons (staff), positions, groups or organisations that will have access to the task. DO NOT set access to individual names of people. This makes it very difficult to modify access once a person leaves UWS. You should always choose either a position or group (eg business unit).

**Note:** If a position or group has not been created in TRIM please contact RAMS and requests a position/group to be created. Ensure to include details of staff that should be associated with each position/group.

Select:  
**Restricted to the following locations**

Select your name and click:  
**Remove**

Click:  
**Add**

Customise Access (Multiple) - Update Record Metadata - D11/623066

Access Control

Everyone

Same As Container Record

Restricted to the following Locations (and any of their members)

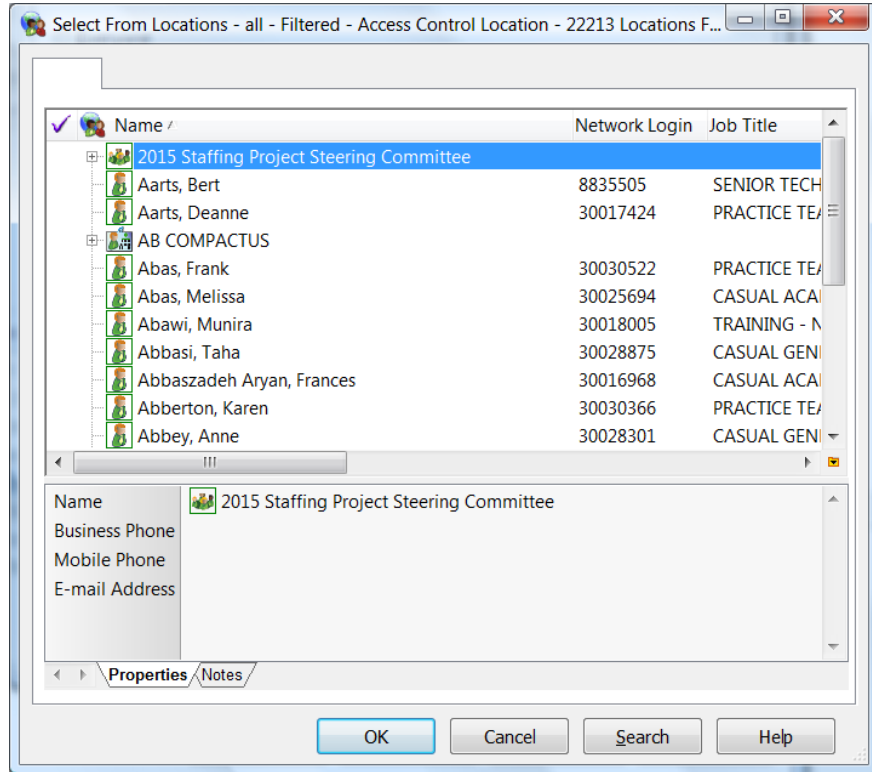
Sort Name

Smith, Michael
----------------

No changes, keep current setting

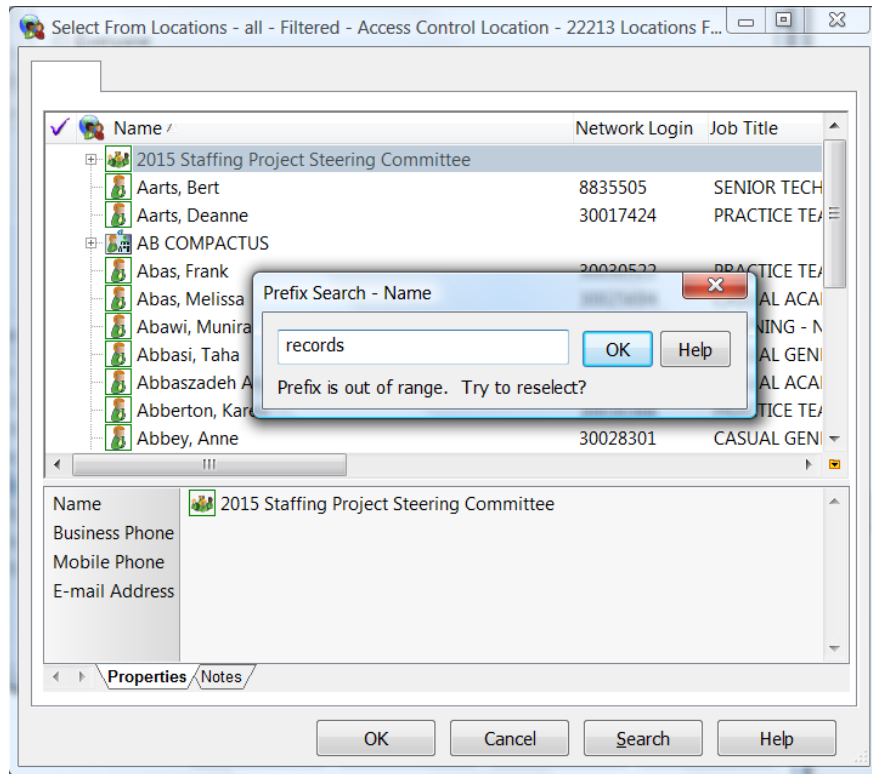
You will be presented with a list of all staff, positions and groups from the University.

**DO NOT** scroll through these. There are tens of thousands.



Start typing the name of the *Position* or *Group* you wish to add for the access.

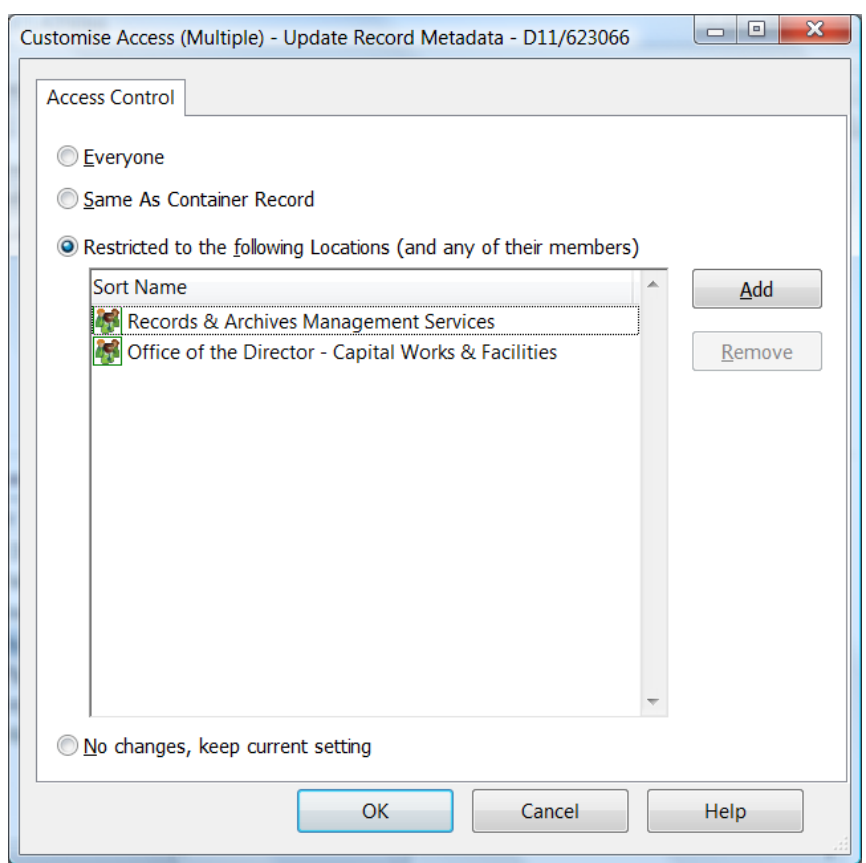
A small window will pop up. You only need type the first three characters but the more you type the smaller the group of results will be.



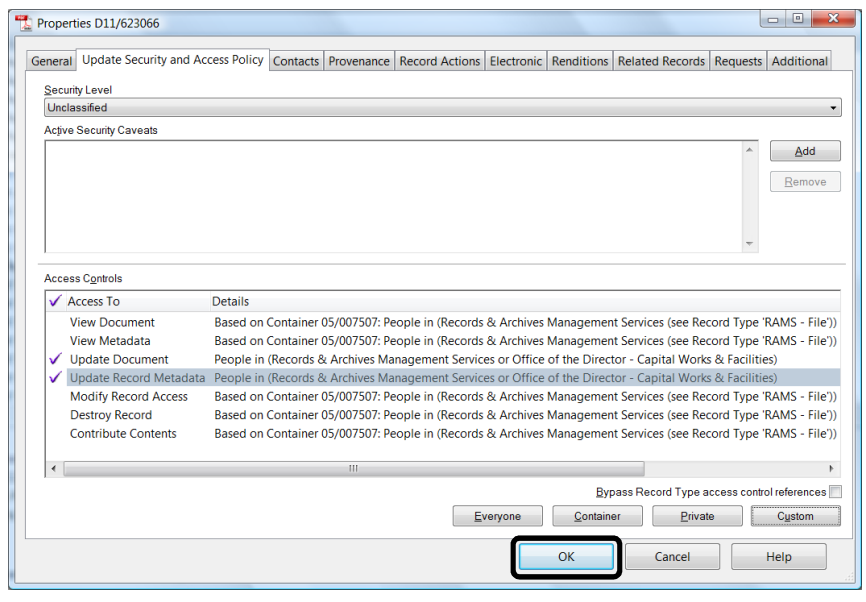
Add:  
- your organisational unit, &  
- Records & Archives Management Services

Click:  
OK

**Note:** Add as many *Positions* or *Groups* as required by clicking on the **Add** button.



Click:  
OK



Due to the sensitive nature of some information being held for legitimate business purposes, the following Document Types have access restrictions built in to ensure information is available to support business, whilst maintaining confidentiality.

Document Types that have specialised access restrictions and **DO NOT** inherit access from files

- BRRG - Notes
- Counselling Service - Document
- Counselling Service - Notes
- Disability Service - Document
- Disability Service - Notes
- Mental Health Assessment
- MHWb - Notes
- Research Service - Research Report
- Student Document - Academic Misconduct
- Student Document - AHEGS
- Student Document - Intl Admissions
- Student Document - Residency
- Student Document - Restricted