TRIM9
Content Manager
Tips & Tricks

Security

Do you deal with confidential records?

Read below to find out how to secure your records!

Knowing how to effectively apply security at the time a file is created ensures our records are appropriately stored with the right people able to access those records when required.

The following rules apply in TRIM:

- Electronic folders created within exisiting cabinet structures will automatically inherit the same security as the cabinets.
- Electronic sub-folders created within electronic folders will automatically inherit the same security as the folders.
- Electronic documents registered within these folders will automatically inherit the same security as the folders.

Understanding UoN's TRIM Security

UoN uses two types of security on our records:

Security Levels

Security levels ensure that records can only be accessed by users who have the same security level or a higher security level than that allocated to the record.

The following outlines the security levels used at UoN:

Higher Restricted This classification applies to highly sensitive information	• Whose unauthorised disclosure could seriously and adversely impact the University, its employees, its students and/or its partner organisations.
Restricted This classification applies to less-sensitive business information	• Whose unauthorised disclosure could adversely impact the University, its employees, its students and/or partner organisations, and • Whose use is restricted to people within the University of Newcastle.

	Note: Information that some may consider private is included in this classification.
Staff in Confidence Refers to the staff of the University, or a business unit or faculty, e.g. Staff – In Confidence, or Human Resource Services – In Confidence	• Information that is related to business unit or faculty operations, but is not available outside the unit or faculty, and • Whose unaythorised disclosure, while against policy, is not expected to seriously or adversely impact the University, its employees, its students and/or its partner organisations. This classification applies to all other information that does not clearly fit into the previous two 'Restricted' classifications.
[No Security Level]	This classification applies to information which: • Requires no special protection or rules for use, and • May be freely disseminated without potential harm.

Please note – users are advised to not use **[No Security Level] as most TRIM users at UoN have a minimum permissions of **Staff In Confidence**.

Access Controls

Access controls allow records to be restricted to particular business units (or people) within the above Security Levels. You can also use access controls to assign control over specific items to specific users.
** Note – Access controls do not define who does not have access, but who does have access to certain records.

The table below lists the seven (7) options for access controls:

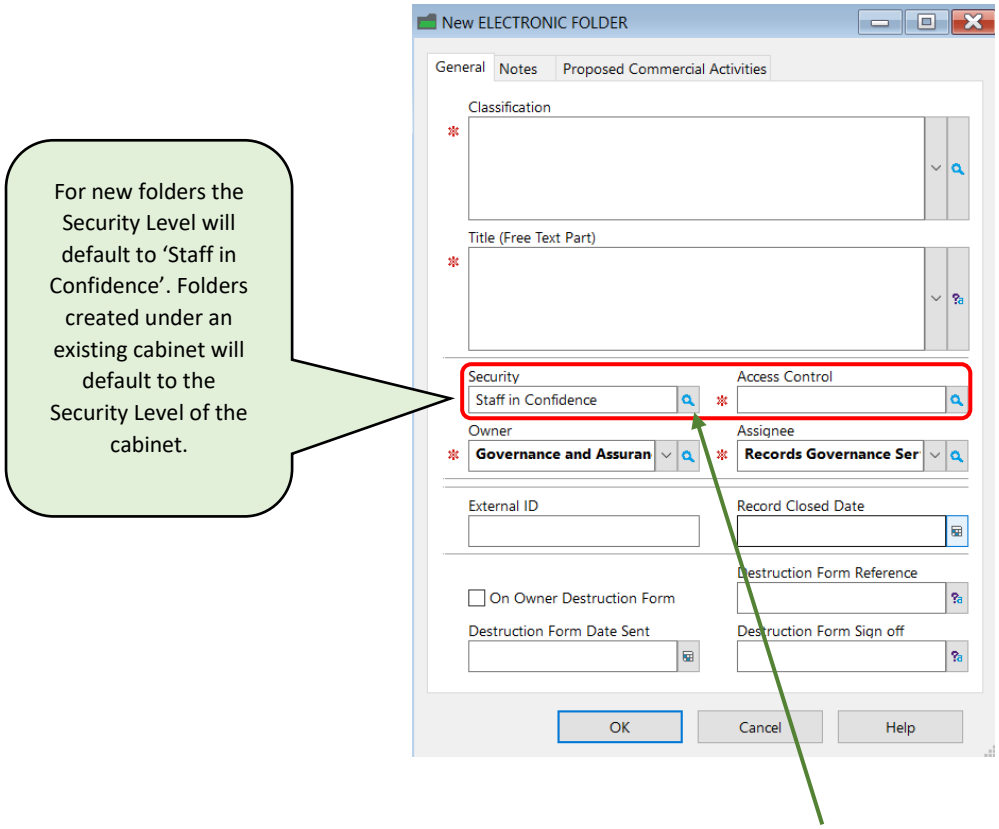
Access Type	Description
View Metadata	Enables users to see a record exists – if a user is not in this access control list, this record will not appear in any search the user may attempt therefore they will not know the record even exists.
View Document	Enables users to view a document attached to a record and view revisions and renditions.
Update Document	Enable users to check out, edit and check in documents.
Update Record Metadata	Determines which users are allowed to change the properities and perform other update tasks on a record – e.g. Title, Author.
Modify Record Access	Determines whether a user can modify the security or access profile of a record to determine who is allowed to modify its access controls.
Destroy Record	Regardless of this setting, users cannot delete records in TRIM unless their permissions allow them. Only system administrators have this ability.

Contribute Contents	Enables users to add contents to the container, regardless of the **Update Record Metadata** access control setting on the container.

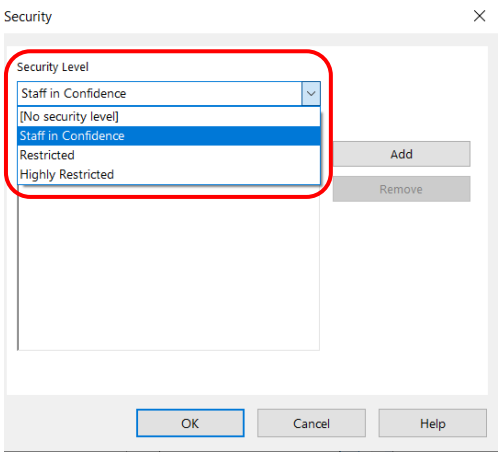
How to Apply Security

To apply security when creating a new folder follow the below instructions:

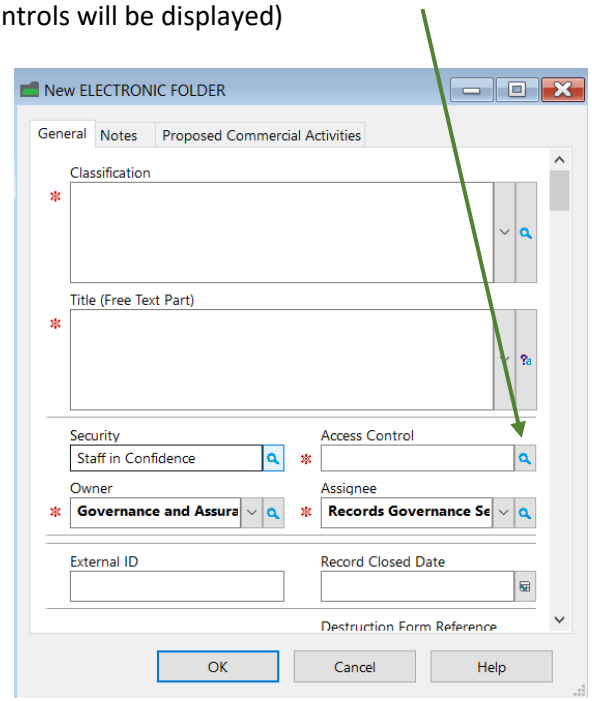
1. On the New Record Metadata form, locate the two security fields below:



2. To change the default security level click the blue Magnifying glass on the Security field and select the required level from the drop-down



3. To change the access controls click the blue Magnifying glass on the Access Control field (the current access controls will be displayed)



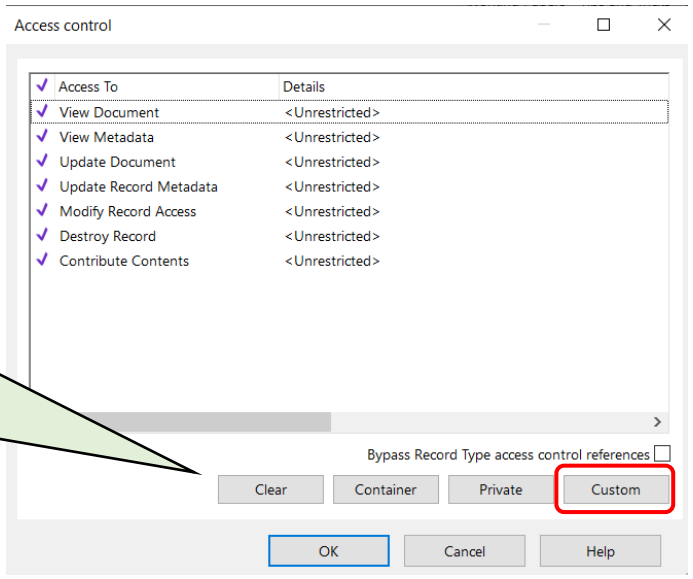
4. To change all criteria to the same access controls, select **ALL** items by placing a tick next to each criteria → Click **Custom** (for all different access contols on different criteriam place a tick next to individual criteria)

Clear: Removes currently access controls that have been selected

Container: Applies the same security as its container (e.g., if the folder is in a cabinet)

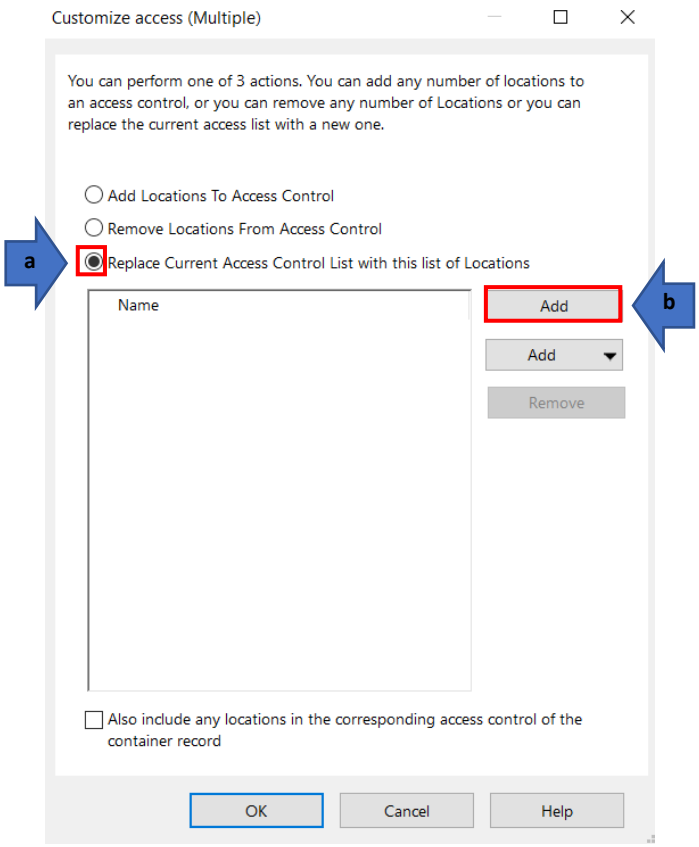
Private: Restricts the folder to just you (not recommended)

Custom: Allows you to select groups of people to have access



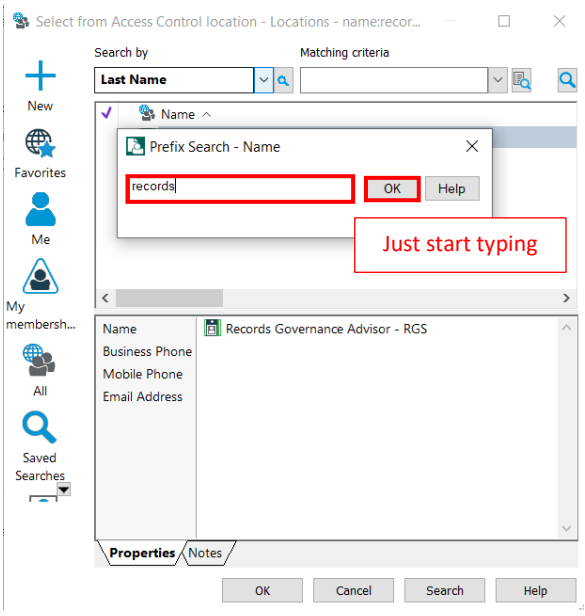
5. In the **customize access (mulitple)** window:

    a. Select **Replace Current Access Control List with this list of Locations**
    b. Click **Add**

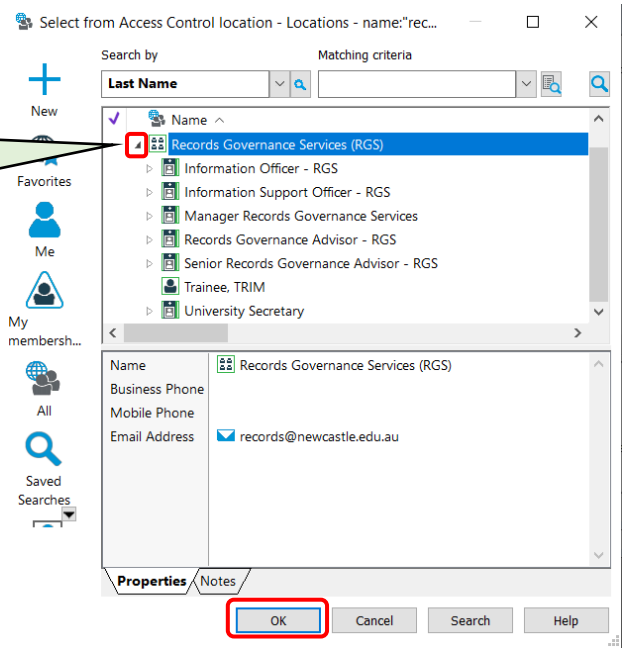


6. In the **Select from Access Control Location** window start typing the name of the location you want to give access to

Note: When selecting a location choose a Green Organisation, Group or Position. Where possible do not select an individual person.

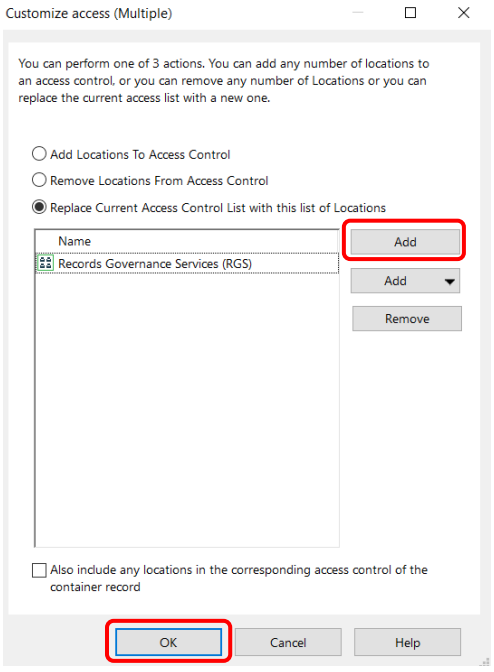


7. Select thye required location → Click **OK**



Note: You can expand the location by clicking on the arrow sign to see the members

8. Click Add and repeat the process to add additional locations to the access controls



9. Click OK when all the required locations have been added

10. Click OK to apply the changes