SECURITY

Do you deal with confidential records? Read below 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 existing cabinet structures will not 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

Security Levels and Access Controls are the two primary types of security used on the University's TRIM 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:

Highly 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 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 College, e.g. Staff – In Confidence, or Human Resource Services – In Confidence	• Information that is related to business unit or college operations, but is not available outside the unit or college, and • Whose unauthorised 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.

NOTE: Users are advised to **not** use **[No Security Level**] as most TRIM users at UoN have a minimum permission 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.

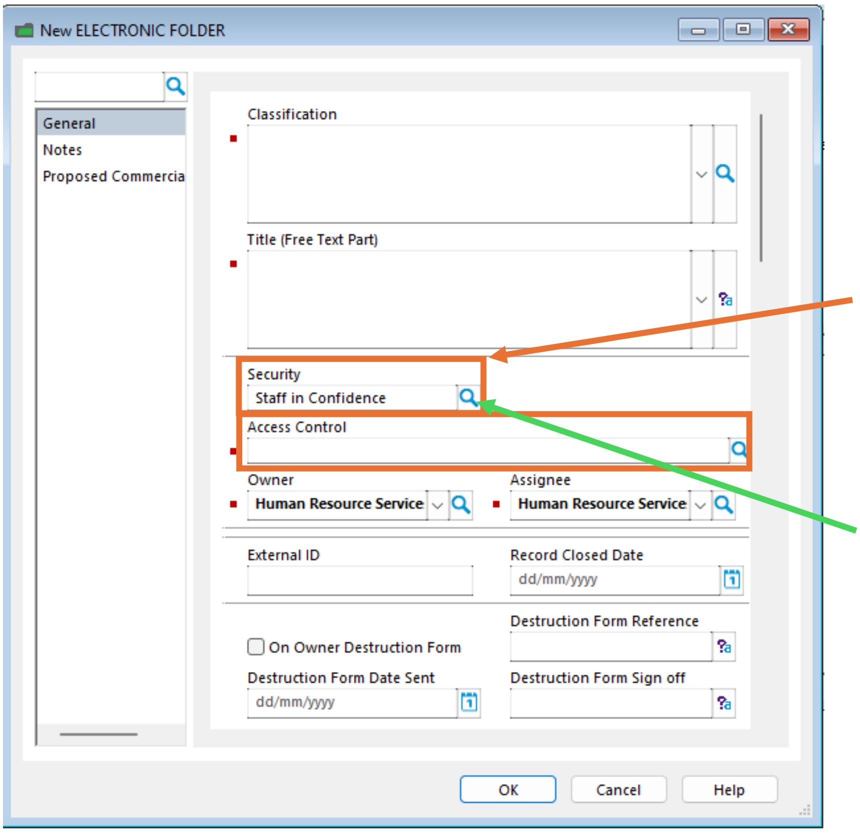
The table below lists the seven (7) options for access controls:

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 properties 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:



New ELECTRONIC FOLDER

Classification:

Title (Free Text Part):

Security: Staff in Confidence

Access Control:

Owner: Human Resource Service

Assignee: Human Resource Service

External ID:

Record Closed Date: dd/mm/yyyy

Destruction Form Reference:

□ On Owner Destruction Form

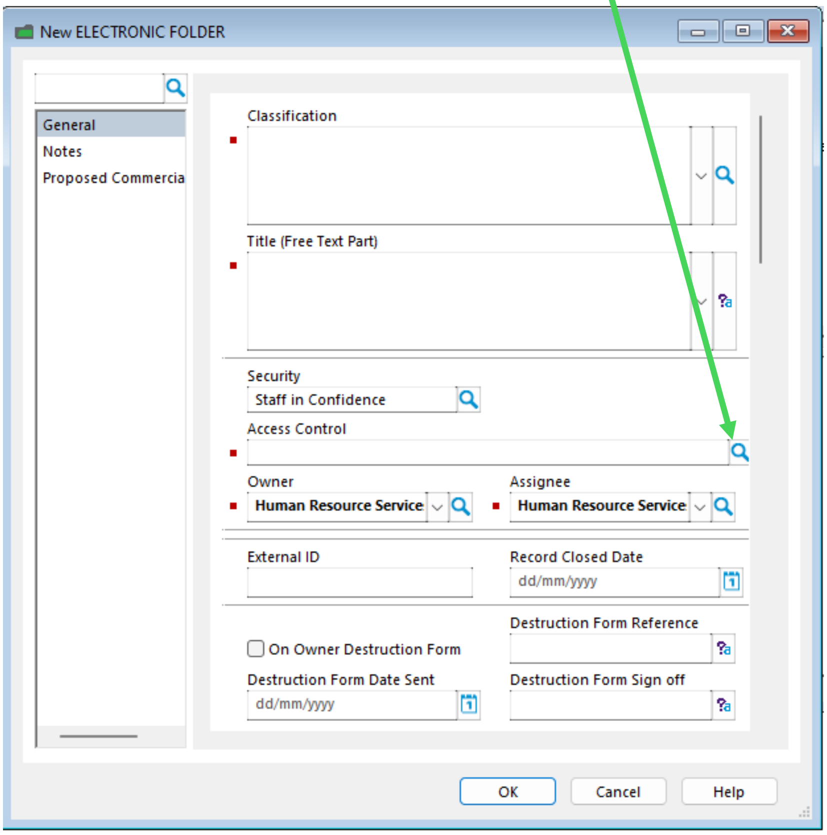
Destruction Form Date Sent: dd/mm/yyyy

Destruction Form Sign off:

For new folders, the security level will default to **Staff In Confidence** (unless the Classification used has a higher security level, in which case that higher security level will be automatically populated here).

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):



New ELECTRONIC FOLDER

Classification

Title (Free Text Part)

Security: Staff in Confidence

Access Control

Owner: Human Resource Service

Assignee: Human Resource Service

External ID

Record Closed Date: dd/mm/yyyy

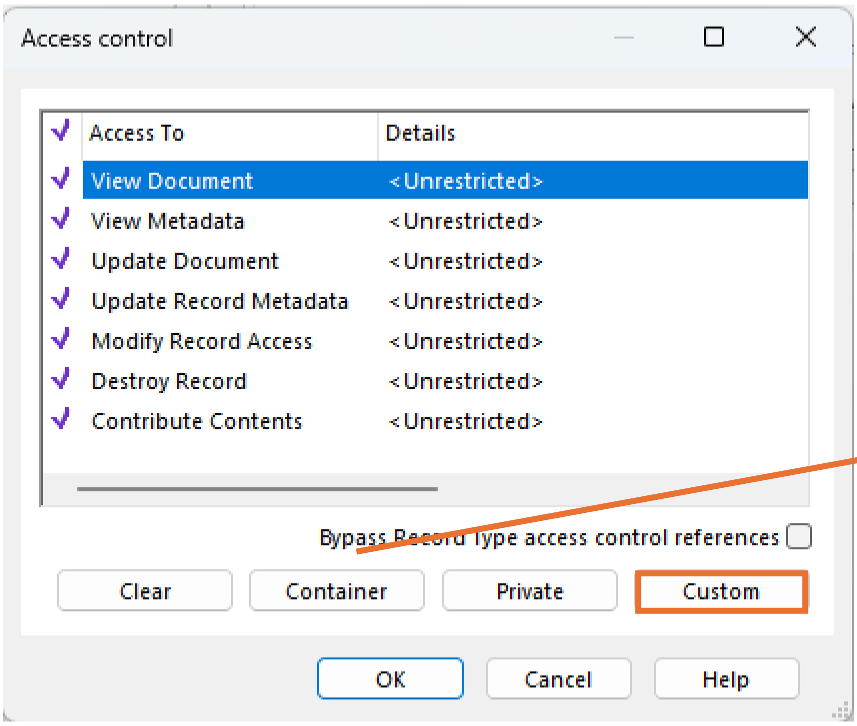
Destruction Form Reference

□ On Owner Destruction Form

Destruction Form Date Sent: dd/mm/yyyy

Destruction Form Sign off

4. To change all criteria to the same access controls, tag ALL items by right-clicking > Select **Tag** All > Click Custom (for all different access controls on different criteria place a tick next to individual criteria):



Access control

✓	Access To	Details
✓	View Document	<Unrestricted>
✓	View Metadata	<Unrestricted>
✓	Update Document	<Unrestricted>
✓	Update Record Metadata	<Unrestricted>
✓	Modify Record Access	<Unrestricted>
✓	Destroy Record	<Unrestricted>
✓	Contribute Contents	<Unrestricted>

Bypass Record Type access control references □

Clear removes current access controls that have been selected

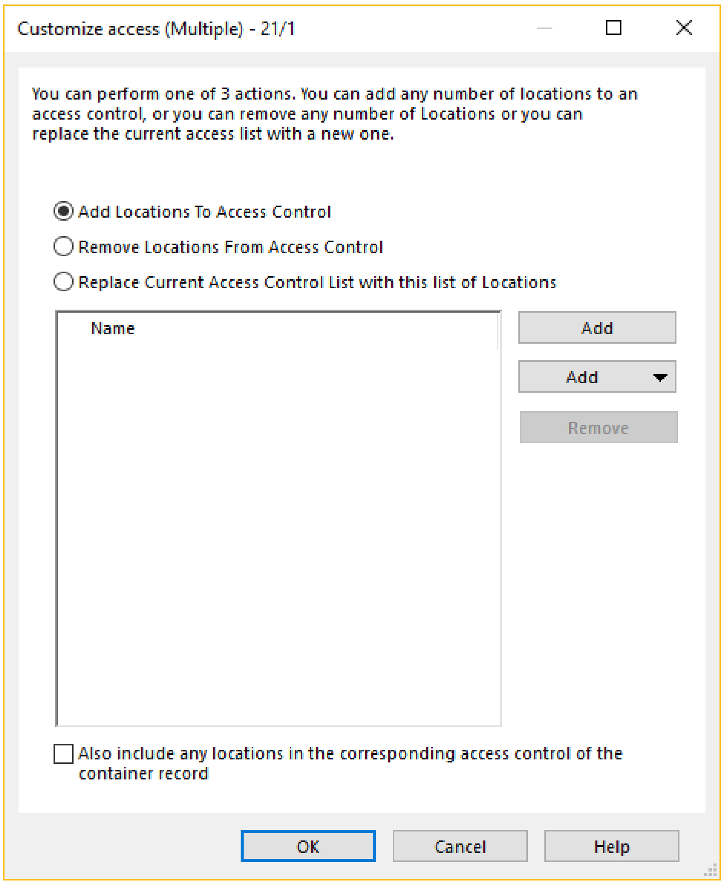
Container applies the same security as its container (e.g., if the folder is in a cabinet)

Private restricts the folder to just you (not recommended)

Custom allows you to select groups of people to have access

5. The **'Customize access'** window will appear. As the below window explains, you can perform one of three actions:
   a. The first option will keep any Locations currently on your selected Access Control(s) (if any) and add in any number of new Locations.
   b. The second option will remove any number of Locations from your selected Access Control(s) (if any).
   c. The third option will replace the Locations currently listed on your selected Access Control(s) (if any) with a new list of Locations.

Select the option you want to perform, then click **Add**:



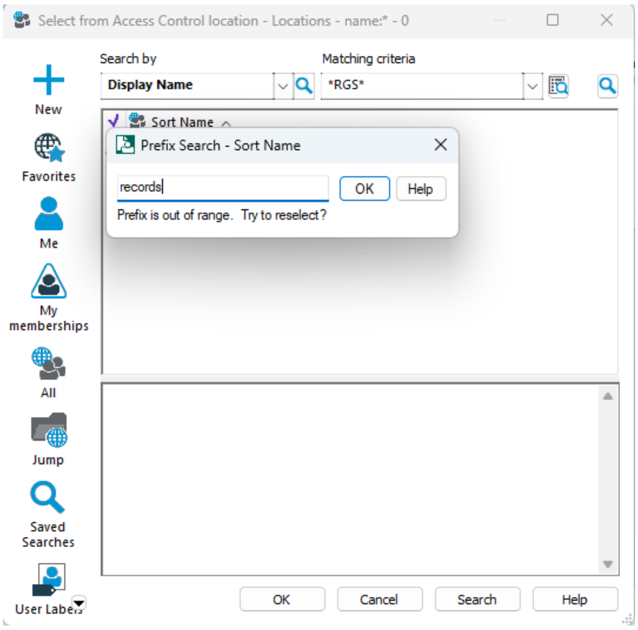
Customize access (Multiple) - 21/1

You can perform one of 3 actions. You can add any number of locations to an access control, or you can remove any number of Locations or you can replace the current access list with a new one.

● Add Locations To Access Control
○ Remove Locations From Access Control
○ Replace Current Access Control List with this list of Locations

□ Also include any locations in the corresponding access control of the container record

6. The **'Select from Access Control location'** window will appear. **Don't click anywhere**, but instead just start typing the name of the Location, Unit/Team you wish to add. When you start typing the **'Prefix Search – Name'** window will pop up. Click **OK** to run the search:



Select from Access Control location - Locations - name:* - 0

Search by: Display Name
Matching criteria: *RGS*

Prefix Search - Sort Name

records

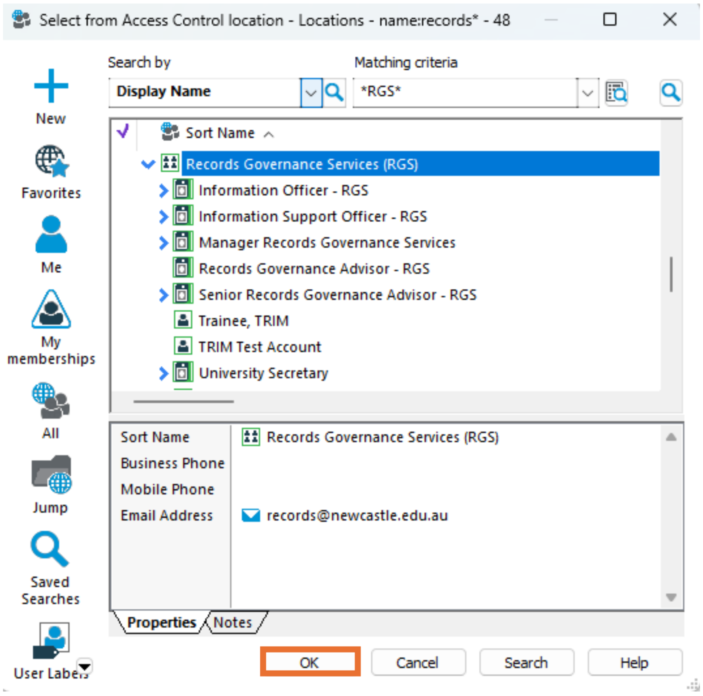
Prefix is out of range. Try to reselect?

Hint: When selecting Locations to grant access to, select:

- A Green **Organisation** Location and/or
- A Green **Group** Location and/or
- A Green **Position** Location

DO NOT select a Person Location because if that person transfers to a different Team, Unit, School, Faculty etc. it will likely be no longer appropriate for them to have access to that folder.

7. Select the required location > Click OK:



Select from Access Control location - Locations - name:records* - 48

Search by: Display Name

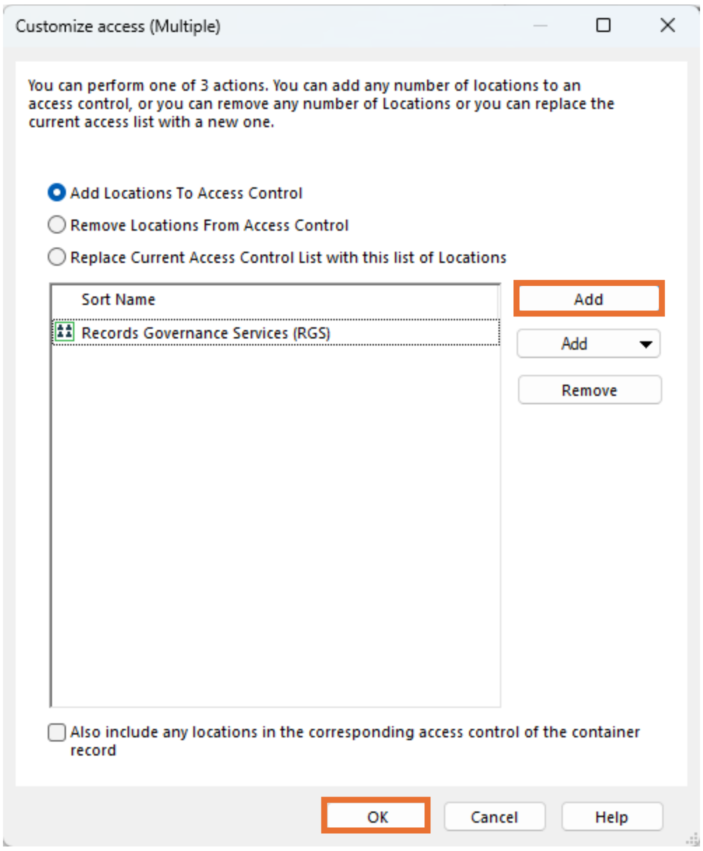
Matching criteria: *RGS*

Sort Name

- Records Governance Services (RGS)
  - Information Officer - RGS
  - Information Support Officer - RGS
  - Manager Records Governance Services
  - Records Governance Advisor - RGS
  - Senior Records Governance Advisor - RGS
  - Trainee, TRIM
  - TRIM Test Account
  - University Secretary

Sort Name	Records Governance Services (RGS)
Business Phone	
Mobile Phone	
Email Address	records@newcastle.edu.au

8. Click **Add** to repeat the process to add additional locations to the access controls. Then, click OK when all the required locations have been added:



Customize access (Multiple)

You can perform one of 3 actions. You can add any number of locations to an access control, or you can remove any number of Locations or you can replace the current access list with a new one.

● Add Locations To Access Control

○ Remove Locations From Access Control

○ Replace Current Access Control List with this list of Locations

Sort Name

Records Governance Services (RGS)

☐ Also include any locations in the corresponding access control of the container record

9. Click OK to apply the changes from the **Access Control** window after all locations have been added.