

Protocols Explained

PROTOCOL FOR STUDENT CASE MANAGEMENT FOLDERS

Records are routinely stored in the student folder relating to the process concerned i.e. undergraduate – Enrolments and Progression

A case management folder may be opened in varying circumstances and may include information that is: highly sensitive; medical; eyes-only; show-cause, etc. or, where multiple processes and units may be involved in managing a particular student issue. Access to case management folders may be restricted to protect privacy and reputation.

Case Management (CM) folders

CM Folders will be opened by the area with the primary role in the case management process or by agreement between two or more areas involved. Where an agreement is reached a designated custodian will be allocated.

CM Folders will be locked down to the areas/officers who require access to the information and/or who are actively contributing to the management of the issue. Access may be broadened on a needs basis.

Access to the CM Folder will be considered on written request to the relevant responsible office as follows: DVC (RI) Office for RHD student matters and DVC (A) Office for all other student records, as required.

The metadata of the CM Folder will be visible for all authorized users to assist them in obtaining and providing advice and in making appropriate referrals etc.

Document Classification types

Within the Case Management folder, people with nominated access will be able to create sub folders containing specific and often sensitive information. When creating or saving information to case management sub folders users should consider the type of information being saved and who should have access to this information. Sub folders can be locked down (Restricted) to certain Faculty/Division/School or Organisational Unit. (Preferably not locked down to individual positions). Once locked down, only those groups with specific access will be able to open or view the folder. It is therefore important that users manually creating case management sub folders ensure that appropriate security and access controls are in place at all times.

Roles and Responsibilities

The area responsible for opening the CM Folder is responsible for assigning permissions.

Staff with access to the CM Folder have a responsibility to manage any personal information in accordance with relevant legislation, including to ensure information gathered for the purpose of case management is only used for that purpose or a directly related purpose.

The area responsible for opening the CM Folder will have responsibility for closing the file once the case has been managed and removing access as appropriate.

Relevant policies

PRIVACY MANAGEMENT PLAN

<http://www.newcastle.edu.au/current-staff/our-organisation/governance/legislation-and-compliance/privacy>

RECORDS MANAGEMENT POLICY - 000285

<http://www.newcastle.edu.au/about-uon/governance-and-leadership/policy-library/document?RecordNumber=D09/1745P>

KEY PRIVACY PRINCIPLES

Section 12 Security and Retention

(a) The information is kept for no longer than is necessary for the purposes for which the information may lawfully be used, and

(c) that the information is protected, by taking such security safeguards as **are reasonable in the circumstances, against loss, unauthorised access, use, modification or disclosure, and against all other misuse**, and...

Section 17 Limits on Use

(b) The other purpose for which the information is used is directly related to the purpose for which the information was collected

Creating a Student Case Management Folder – (ELICOS, International, Enabling, ESOS, & Res-Life)

Note! RHD staff will use the Case Management Folder within their RHD cabinet

1. In TRIM search or navigate to the Student Cabinet
2. Open the Student Cabinet
3. Scroll down and highlight the Case Management Folder

Record Number	Title
8529633/17	RHD - TEAK Anne 8529633
8529633-16	Academic Support - TEAK Anne 8529633
8529633-15	Case Management - TEAK Anne 8529633
8529633-14	Admissions - TEAK Anne 8529633
8529633-13	Enrolment and Progression - TEAK Anne 8529633
8529633-12	Credit - TEAK Anne 8529633
8529633-11	Careers and Student Development - TEAK Anne 8529633
8529633-10	Fees and Financials - TEAK Anne 8529633
8529633-09	Scholarships and Prizes - TEAK Anne 8529633
8529633-08	Placements and Practicums - TEAK Anne 8529633
8529633-07	Exams and Assessment - TEAK Anne 8529633
8529633-06	Graduation - TEAK Anne 8529633
8529633-05	Student Life and Activities - TEAK Anne 8529633
8529633-04	Accommodation - TEAK Anne 8529633

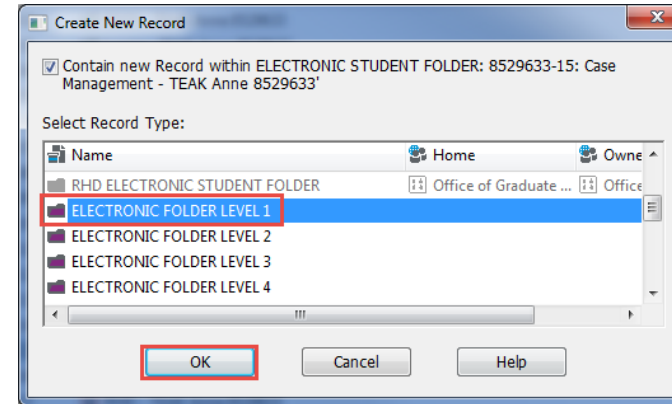
4. Right-click > **New** > **New Record**

Record Number	Title
8529633/17	RHD - TEAK Anne 8529633
8529633-16	Academic Support - TEAK Anne 8529633
8529633-15	Case Management
8529633-14	Admissions - TEAK
8529633-13	Enrolment and Pro
8529633-12	Credit - TEAK Anne
8529633-11	Careers and Studer
8529633-10	Fees and Financials
8529633-09	Scholarships and P
8529633-08	Placements and Pr
8529633-07	Exams and Assessm
8529633-06	Graduation - TEAK
8529633-05	Student Life and A
8529633-04	Accommodation -

Right Click on
Case
Management
Folder

Tag All Ctrl+A
 Untag all Ctrl+U
 Invert all tags
 Copy Ctrl+C
New > **New Record**
 Search
 Navigation
 Contained Records
 Details

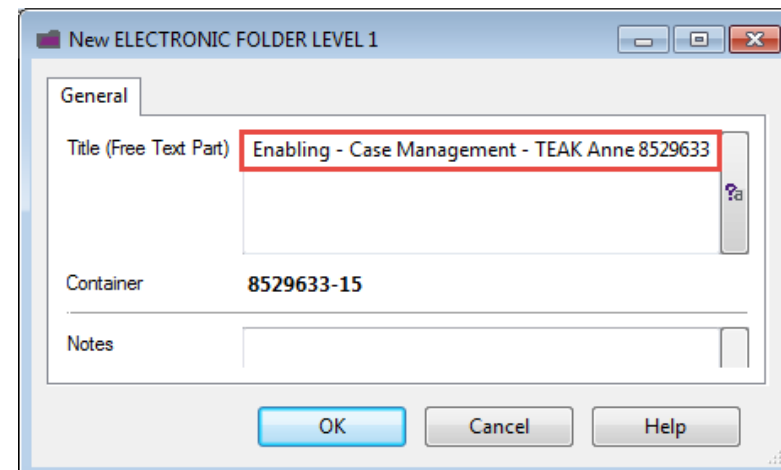
5. Select Electronic Folder Level 1



6. Enter the title as per the Naming Convention

- Enabling - Case Management - TEAK Anne 8529633
- RESLife- Case Management - TEAK Anne 8529633
- ELICOS - Case Management - TEAK Anne 8529633
- International - Case Management - TEAK Anne 8529633

7. Click OK



Changing Access Controls

By **default** documents and sub folders will **inherit** the **Access Controls** from the File they are placed in and if moved to another File it will **inherit** the **Access Controls** from the new file.

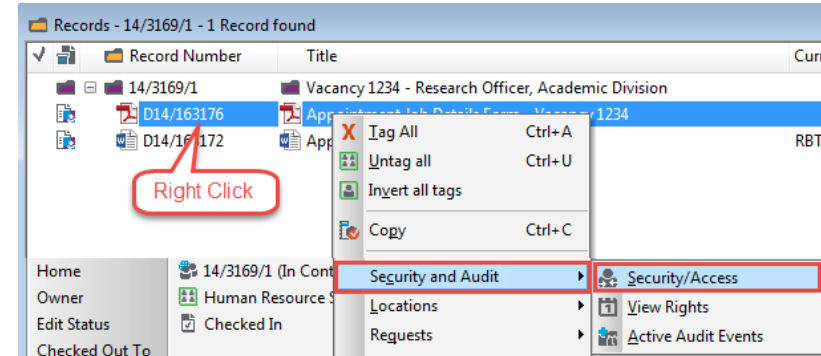
You can use Access Controls to assign control over specific items to specific users. Access Control does not define who does not have access, but who does have access to certain records.

The table below lists the seven (7) options for Access Controls

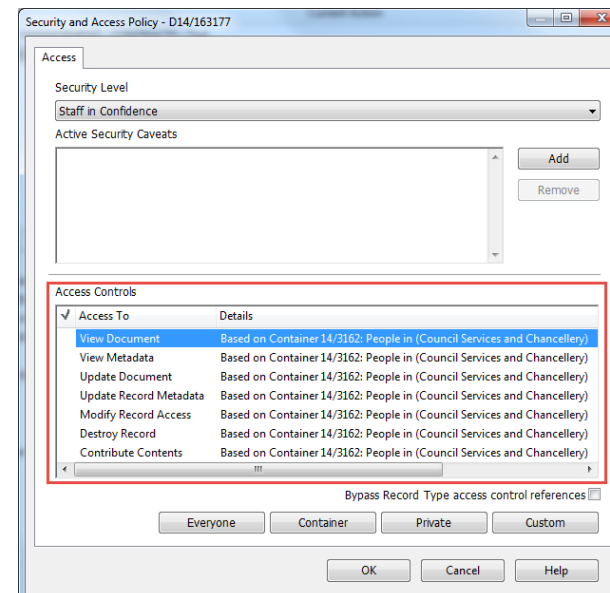
Access Type	Description
View Metadata	Enables users to see a record exists - If a user is not in this Access Control list, this record will not appear in any search the user may attempt therefore they will not know the record even exists
View Document	Enables users to view a document attached to a record and view revisions and renditions
Update Document	Enables 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 etc.
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 user 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

Locate the sub folder or document

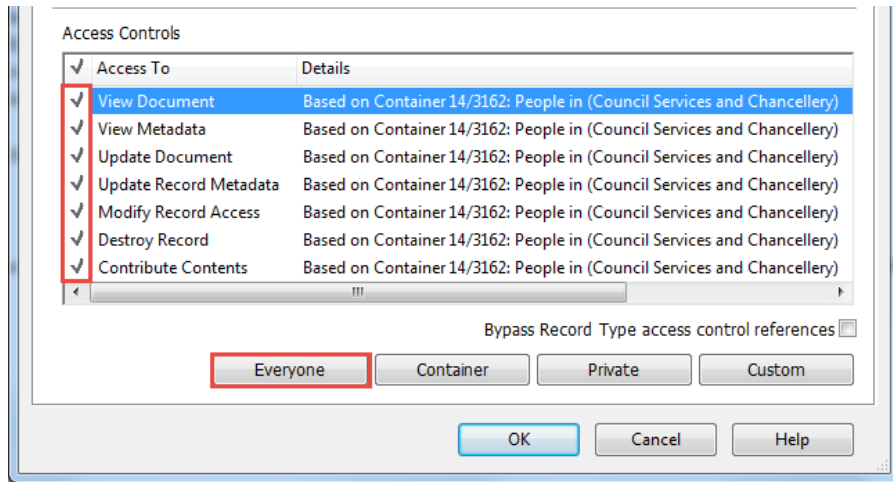
1. **Right Click**
2. Select **Security and Audit**
3. Select **Security/Access**



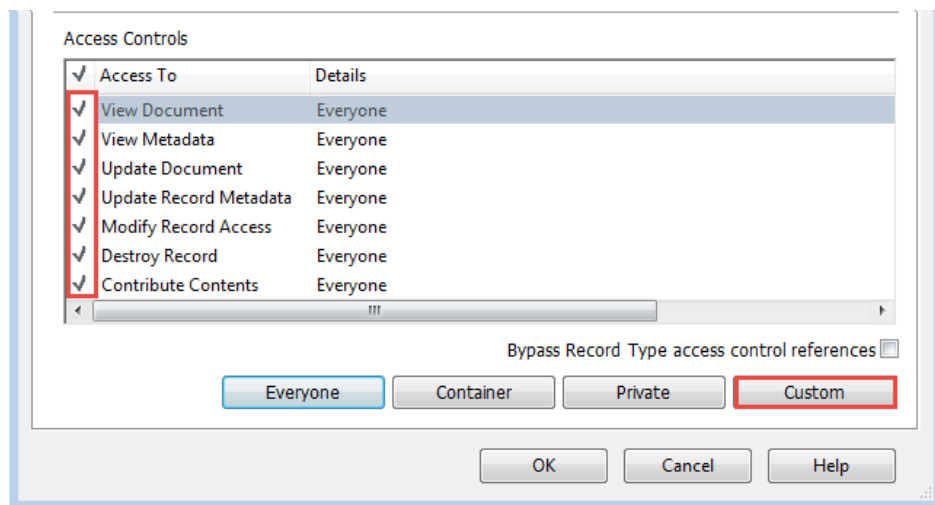
The current Access Controls can be seen in the lower half of the Security and Access Policy window



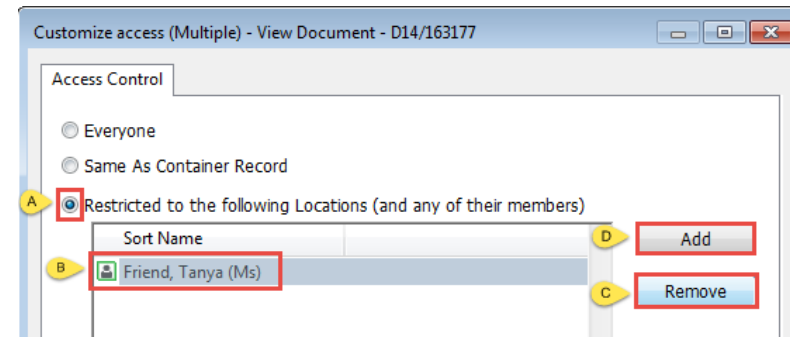
4. Select **ALL** items by placing a **tick** next to each one
5. Click **Everyone** (You must first remove the document or sub folder from being 'Based on Container')



6. Select the required access options by placing a tick next to each one (refer to the above table for details of each option)
7. Click **Custom**






8. In the Customize access window
 - a. Select **Restricted to the following Locations (and any of their members)**
 - b. Highlight **your name** in the list
 - c. Click **Remove**
 - d. Click **Add**



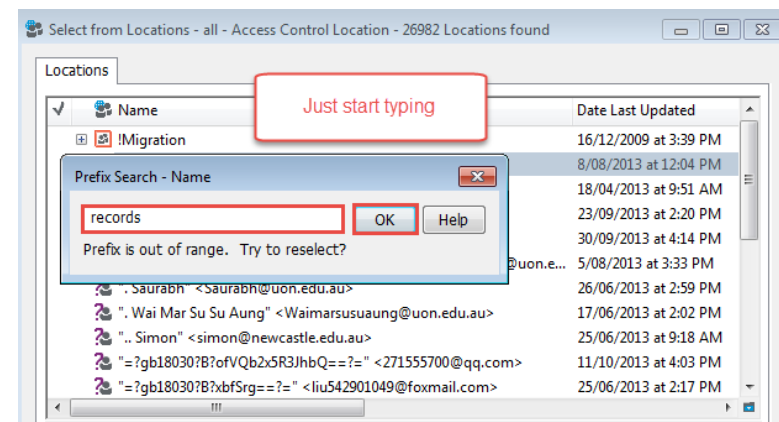
The **Select from Locations** window will appear

Just start typing the name of the **location** you want to give access to

Note! When selecting Locations to allow Record access, select a Green 

Organisation or  group. Where possible, **do not** select a  Person. If an organisation or group does not exist please contact your Administrator.

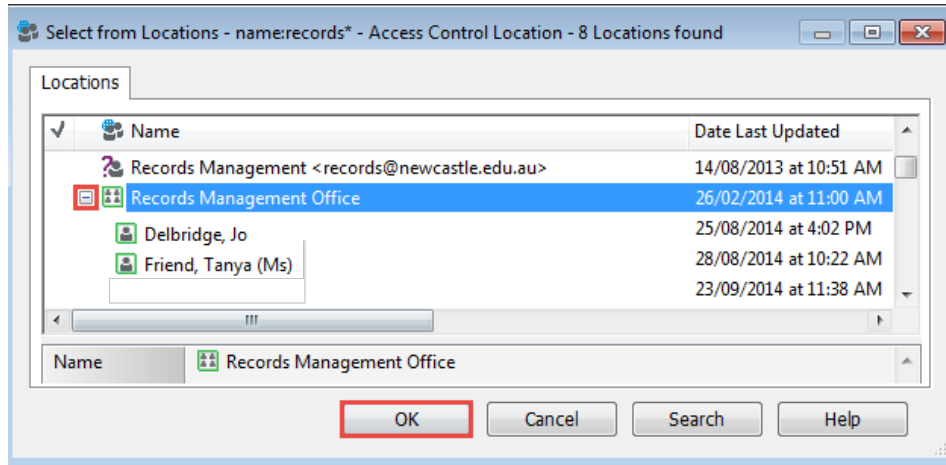
9. Click **OK**



10. Select the required **location**

Note! You can expand the location by clicking on the + sign to see the members

11. Click OK



12. Click **Add** and repeat the process to provide access to additional groups

13. Click **OK** when all the required groups have been added

