New user: IT induction process

Version: 1.2

Issued: 9th April 2020

Author: Jon Rolph

Document Control

Date	Ver	Change Description	Author
05/01/2019	0.1	Initial document created	Jon Rolph
16/01/2019	0.2	Include detail of new Hardware Request workflow	Damian Cutler
13/02/2019	0.3	Update of Hardware Request form and process	Damian Cutler
20/02/2019	0.4	Update Access Request icon	Jon Rolph
23/05/2019	1.0	Update CEO details and first endorsed version	Jon Rolph
10/03/2020	1.1	Updated to include Data Dashboard & Power BI licencing, create user from existing user, Form Creator Access and User is a Delegate.	Damian Cutler
09/04/2020	1.2	Updated to include options to mark account active after being disabled and ability to delete duplicate accounts.	Damian Cutler

Authorisation

Name	Position	Signature & Date
Reuben Robinson	CEO Galambila	
Robert Skeen	CEO Biripi	
Chris Spencer	Interim CEO Tobwabba	
Alicia Stewart	Acting CEO Durri	
Fay Adamson	CEO Werin	

Index of this document

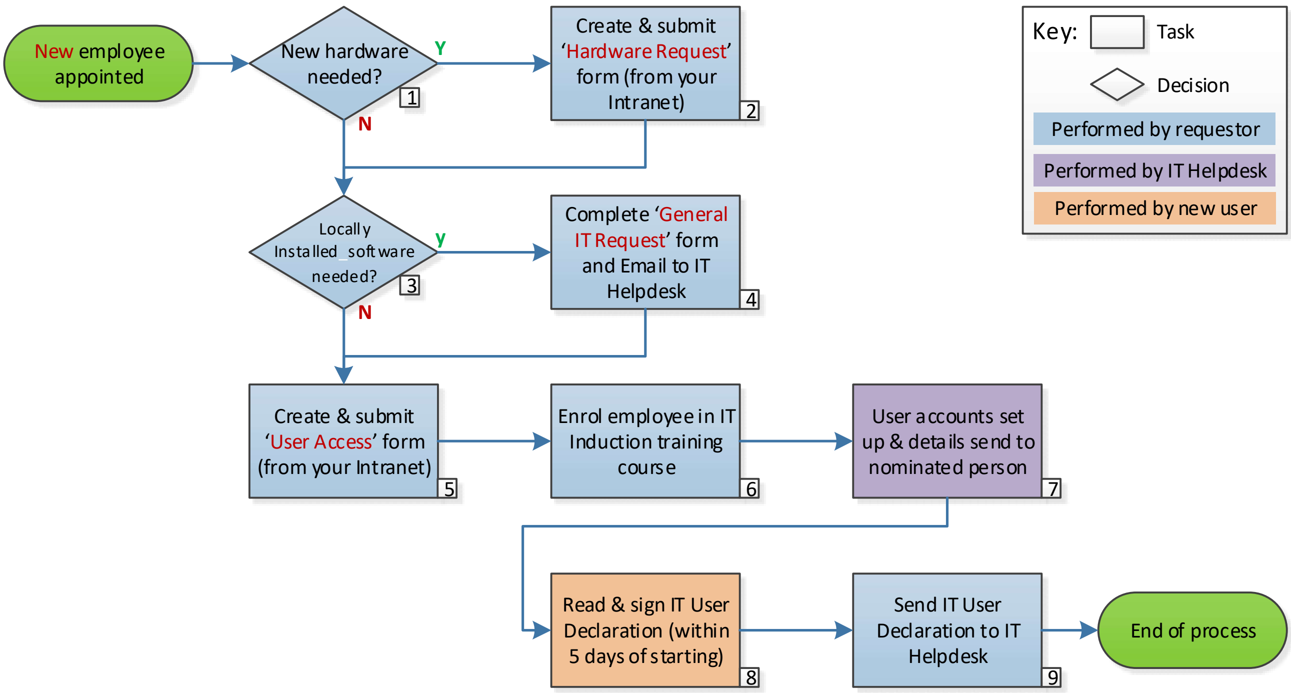
Introduction

To provide a secure and efficient IT service it is vital that all users of the service have:

- The right equipment
- The right software
- The right levels of access
- The right knowledge

This process is designed to ensure that these requirements are achieved for new staff and other users who will be provided with access to IT Services.

Overview of process



Detail of each step in the process

The following outlines the steps to be followed when a new employee is engaged:

1. New hardware needed?
   As a general rule, if a new employee is taking over the role of another, the existing IT hardware will be inherited by the new employee.
   Where an employee is performing a new role, or is an additional member of staff performing an existing role, then additional hardware is likely to be needed.
   If in doubt please contact the Regional IT Manager (email: it.manager@galambila.org.au or call: 6652 0850)

2. Create & submit 'Hardware Request' form
   If new hardware is needed requirement should be documented through the "Hardware Request" form located on your intranet site. The icon used for this is below:

   (Details of how to complete this form are contained in Appendix 1 at the end of this document.)

   The request will be reviewed by the Regional IT Manager, who will provide any equipment needed. In doing so he will consider the following:

   a. Is there existing equipment that can be reallocated?
      The remit of IT@RAMS is to provide the IT equipment needed to support the core services of each of the organisations within the IT@RAMS consortium. Where appropriate this can include the reallocation existing equipment, both within and between organisations.

   b. Should a third party be covering the cost of the equipment?
      For non-core services (e.g. programmes, projects, etc) IT@RAMS is not responsible for funding IT equipment. In exceptional circumstances, such as unfunded programmes where there is great patient need, the IT@RAMS consortium management committee may approve an exception to this.
      Where the cost is to be covered by a third party, IT@RAMS will purchase the equipment and then re-charge the cost to the appropriate cost centre.

   If agreed by the Regional IT Manager, equipment will be ordered and provided to the new staff member.

3. Locally installed software needed?
   Each computer will include the following software:

   - MS Office 2013 Professional
   - Outlook
   - Adobe Reader
   - Windows Media Player
   - PDF Creator

   If the new employee is to perform a role that requires other software, for example; advanced graphics, desktop publishing or project management, it may need to be purchased (the Regional IT Manager can advise on this).

4. Complete General IT Request form and Email to IT Helpdesk
   A request for additional software would be submitted using the General IT Request form, found in your local G: drive.
   G:\DRV - ?? - General\IT\Forms (where ?? are the two letter short name for your site)

Generally the individual organisation will be responsible for the cost of purchasing and installing any local software.

Note: information on how to complete the General IT Request for can be found in a guide in your local G: drive.

G:\DRV - ?? - General\IT Processes & Procedures (where ?? are the two letter short name for your site)

5. Create & submit 'User Access' form
   Setting up a new account and allocating access levels to it is done through an online form that can be found on the main page of your intranet site. The icon used to identify the form is below.

   (Details of how to complete this form are contained in Appendix 2 at the end of this document.)

6. Enrol employee in IT Induction training course
   IT@RAMS have developed a short online training course to introduce new users to the most important initial information related to the IT service.
   The course is available for all new users and can be accessed either prior to commencement or as part of a staff induction programme at commencement.
   The training can be initiated by IT@RAMS (email it@galambila.org.au) or the HR function at each organisation.
   This training course is intended as a basic introduction only. Additional training will be provided by IT@RAMS, specific to the role of the individual, following the completion of the induction training course.

7. User accounts set up & details send to nominated person
   The IT Helpdesk will create a new user account, based on the approved access. The login details for the account will be sent to the person who requested it. They are responsible for keeping this information safe until it is passed to the new employee.

8. Read & sign IT User Declaration
   IT@RAMS has a set of "rules" to be followed if an employee is to have IT services. The rules are embedded in a declaration which the employee should read, understand and then sign.
   The Declaration can be found on your G: Drive in the following location:

   G:\DRV - ?? - General\IT\Forms (where ?? are the two letter short name for your site)

   If there are any questions related to the declaration contact the Regional IT Manager.

9. Send IT User Declaration to IT Helpdesk
   The signed IT Declaration should be scanned and emailed to the IT Helpdesk (email: ithelpdesk@ramsits.com.au).
   If the signed IT declaration is not with the IT Helpdesk within five working days of the first login access to the account will be suspended.

Appendices

Appendix 1: Hardware Request Form Completion Guide

Please refer to the following guide when completing the Hardware Request form:

Step 1: Open Request New IT Assets Form

Select "Request New IT Assets" from the IT Assets page of your intranet site. The icon used to identify the form is below. (Icon colours vary between sites)

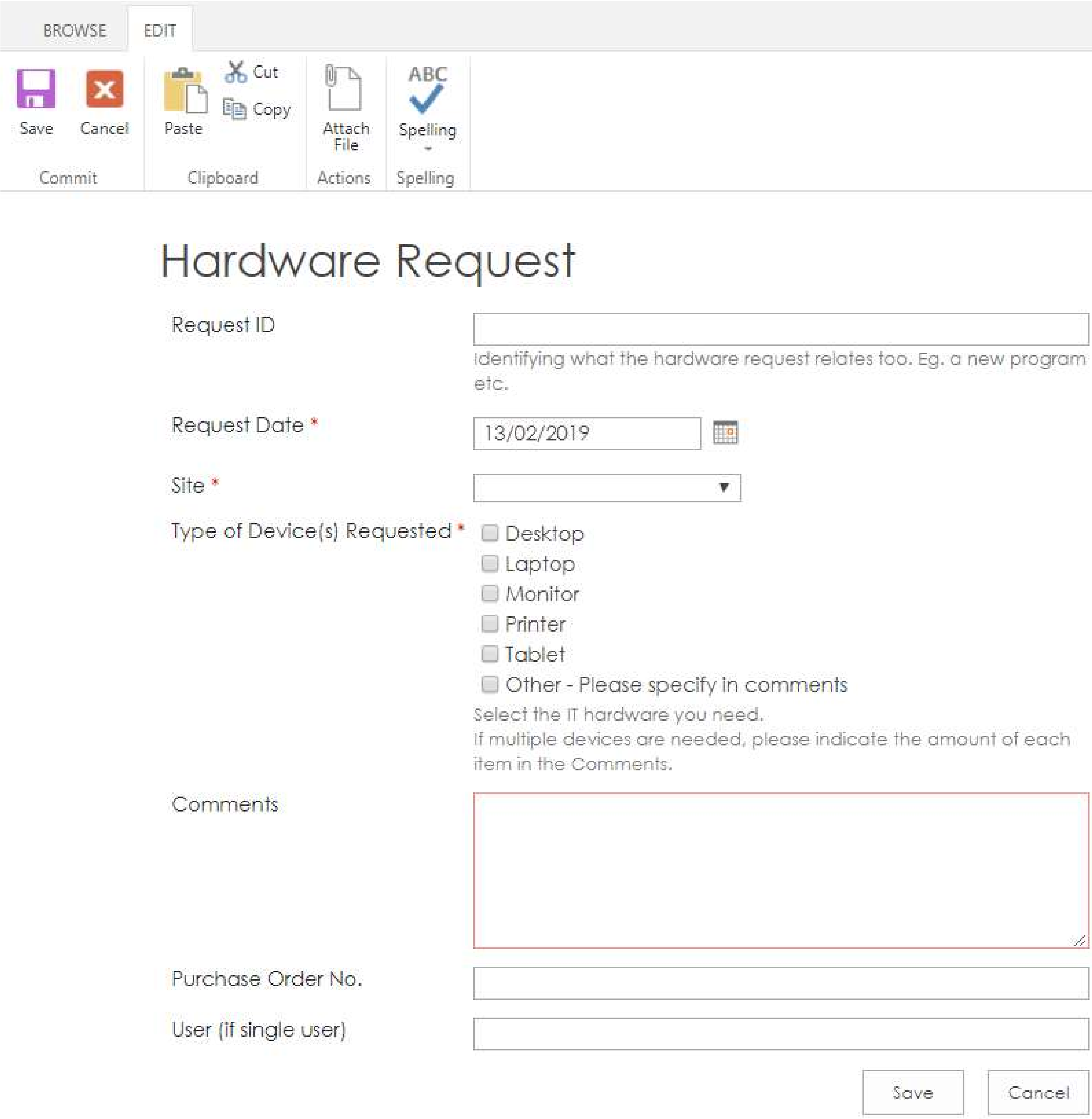
Step 2: Enter Request Details

Enter the details of the hardware request. The fields required are:

- Request ID: Enter a value to help identify what the requested hardware is for. Eg. New laptop for outreach clinic, new program etc.
- Request Date *: Request date is the current date by default.
- Site *: Select your site from the list.
- Type of device requested *: Select the device type from the 6 options of Desktop, Laptop, Monitor, Printer, Tablet or Other. If you are requesting multiple device types, you will need to tick the required devices and indicate how many of each in the Comments field.
- Comments: Enter any comments applicable to the hardware request including number of devices if multiple are required. This is also where you can request wireless mouse for laptop, laptop bag etc.
- Purchase Order No.: Enter your purchase order number for the hardware request if applicable.
- User (if single user): Enter the name of the user that the hardware is to be allocated to. Only complete if the hardware is for a single user.
- Attachments: Add attachments to the hardware request. This may include brochures etc. for the requested hardware. This is located above the form in the standard view.

NOTE: Any field with an asterisk (*) is a required field and must be completed to submit the request.

Once all the fields have been completed, click on the save button to send to the Regional IT Manager for review. If agreed by the Regional IT Manager, equipment will be ordered and provided to the new staff member.


BROWSE | EDIT

Save | Cancel | Paste | Cut | Copy | Attach File | Spelling

Commit | Clipboard | Actions | Spelling

Hardware Request

Request ID

Identifying what the hardware request relates too. Eg. a new program etc.

Request Date * 13/02/2019

Site *

Type of Device(s) Requested *
- Desktop
- Laptop
- Monitor
- Printer
- Tablet
- Other - Please specify in comments

Select the IT hardware you need.
If multiple devices are needed, please indicate the amount of each item in the Comments.

Comments

Purchase Order No.

User (if single user)

Save | Cancel

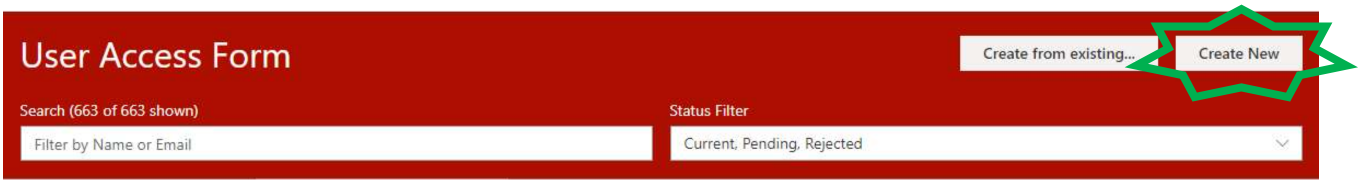
Appendix 2: New employee 'User Access Form' Completion Guide

Please refer to the following guide when completing the form for new employees:

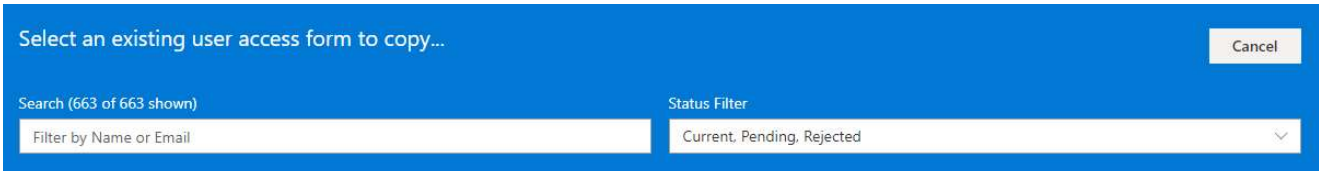
Step 1: Open a new form or copy an existing form

Select the "User Access Form" from the main page of your intranet site. The icon used to identify the form is below.

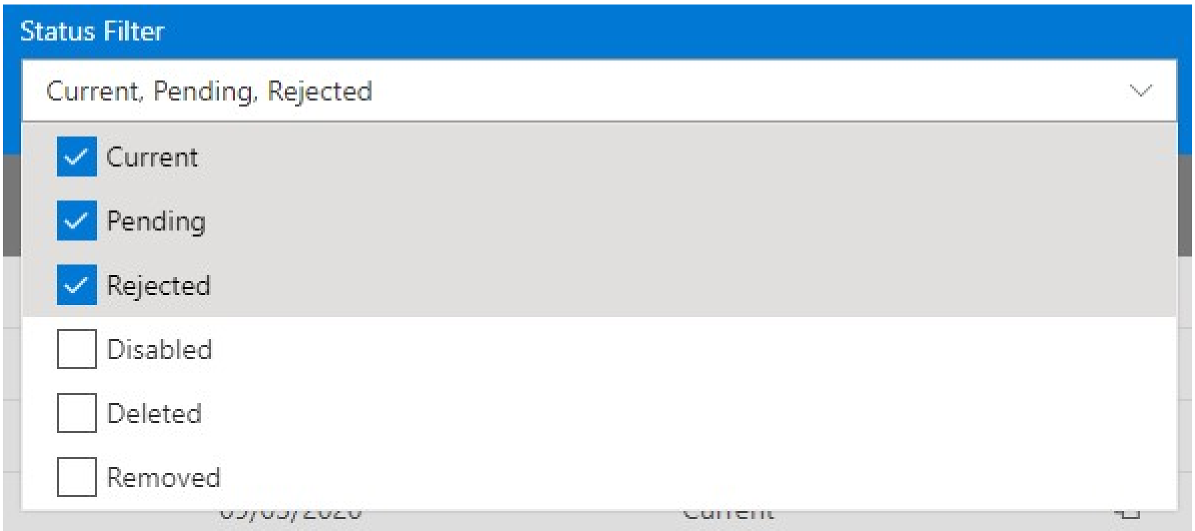
At the top of the page select "Create New" to start out with a blank User Access Form,



Or select "Create from existing" to search for a current user and copy their access.

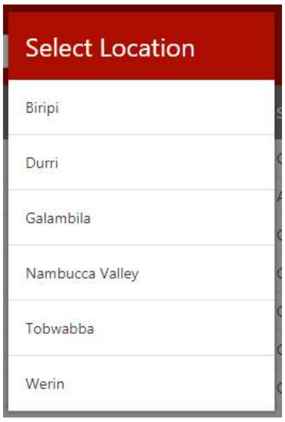


You can also filter users for your organisation by their account status.



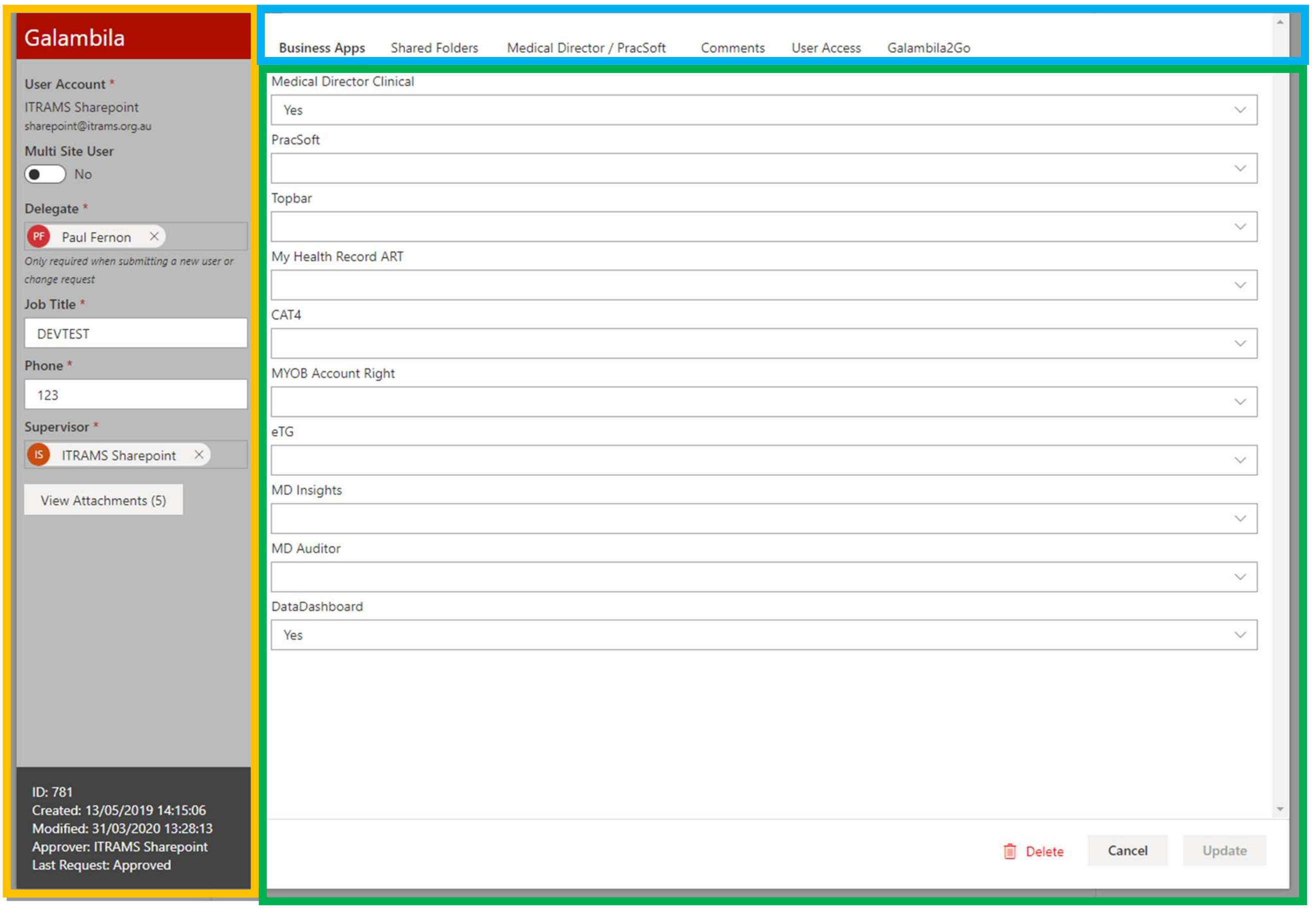
Step 2: Select the location for the user

Select the location where the user usually works. There is an option (see later) where a user can be granted access to IT services at more than one location. At this stage just identify the main location.



Step 3: Enter details for the user

The User Access Form consists of a number of pages that cover all aspects of the access to be granted. The details of each page will vary depending on the location selected in step 2. The general format, however, is common and shown below.



The sidebar (in yellow) contains the personal details whilst the main window (in green) contains a number of tabs (in blue) that represent different aspects of the user's access.

Step 3a: Enter personal details for the user

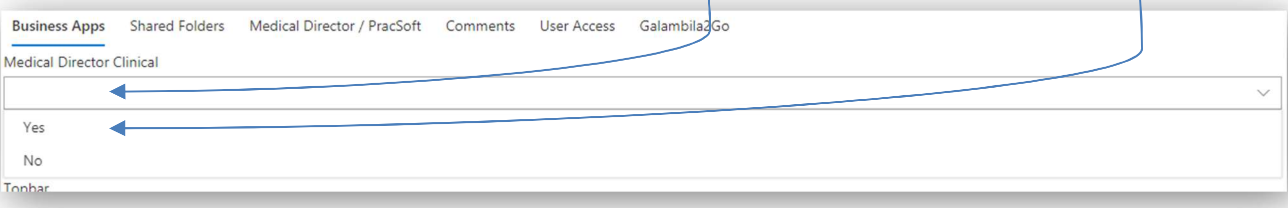
The sidebar (in yellow) must be completed for all requests as below:

- Name: The name of the user, written as first name and surname with a space between each. This will be used by the IT Helpdesk as the basis of the user account name and email address so please ensure this is spelled correctly!
- Multi Site User: Where a user will work at multiple sites (e.g. a visiting specialist) they can use the same logon name and password for all if they are identified as multi-site users.
  NB: A new Access Form must be created for each site, identifying that the user will access multiple sites. The IT Helpdesk will then combine all the approved requests into a single account.
- Delegate: This is the name of the IT delegate who will approve the request. Select the delegate from the drop down list of approvers for the site.
- Job Title: This will appear in the person's contact details, so a consistent and accurate title will help colleagues to know who the new user is.
- Phone: The phone number will also be available within the employee's contact details.
- Supervisor: This is the person who will receive the login details when the new user account is set up. Knowing the supervisor also helps build up an organisational structure within the IT systems.

Step 3b: Enter remaining details for the user

Whilst the exact details to be entered are different for each organisation, reflecting the different applications used by each, the method of doing this is common to all.

For each option that you want to include, click on the rectangle below the name and select "Yes".



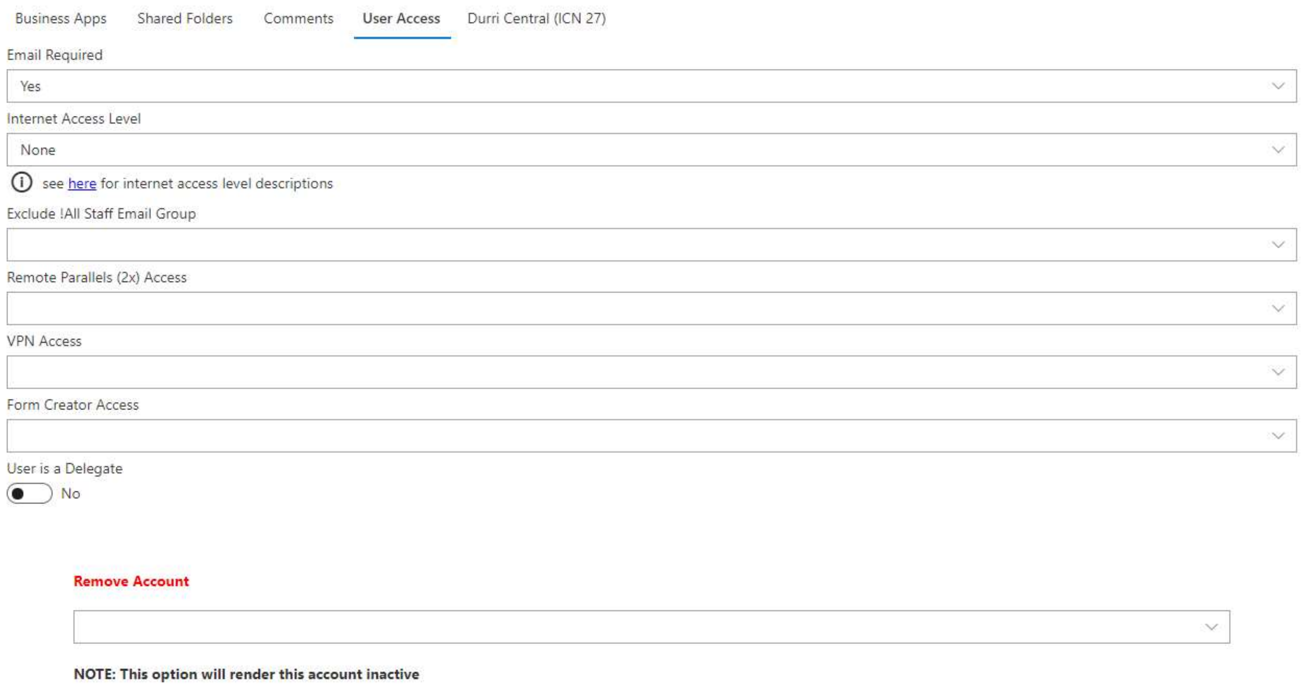
Repeat this for all fields that are required.

Note: you can select "No" where access is not to be granted. The Helpdesk will, however, assume that blanks are not approved.

Note: The Data Dashboard application requires a Power BI licence which is charged per user. This cost will be recharged to each organisation monthly.

Step 3c: Complete the User Access tab

The "User Access" tab requires some explanation and is common to all organisations. I will therefore provide more detail on filling in this element of the form:



Each entry is outlined below:

- Email Required: For some account (e.g. visiting specialists) there is no benefit in having an email account.
  NB: Since the vast majority of users have an email account, if this is left blank an email account will be added.

- Internet Access Level: Ensuring that staff have only the level of internet access they need for their role, and no more, is a way of minimising the risk of malware infection through compromised web sites. There are six levels of access (other than no access) that is supported. Pick the most appropriate one from the list:

  None: No internet access is provided

  Base: Access to the most common types of web site and suitable for most users

  Shopping: As Base PLUS shopping web sites

  Education: As Shop PLUS streaming media web sites

  Social: As Education PLUS social media web sites

  Webmail: As Stream PLUS web based email (often used for Registrars or visiting specialists)
  Note: Access to work email via the Office 365 web site does not require this

  The following link will take you to a detailed list of the types of site available to each level: http://itrams.org.au/resources/Zscaler%20Internet%20Access%20Levels%202020.pdf

- Exclude !All Staff Email Group: Each organisation has a public group that will send emails to all staff. Some account, such as visiting specialists, Board members, etc. would generally be excluded from this group so they do not receive such emails.

- Remote Parallels (2x) Access: Parallels, formally called 2x, is the system through which most shared applications are accessed. To protect our confidential information access to such systems is prohibited from anywhere physically outside the organisations without special permission. Selecting this option will give such permission.
  Note: This option required the use of a 2 factor authentication, which will be provided by the IT Helpdesk.
- VPN Access: The VPN (Virtual Private Network) client is a way of securely connecting to some IT services when working remotely, via an IT@RAMS provided computer. The services that will be accessible via a VPN connection are; Network drives, Printers and Parallels delivered applications (e.g. Medical Director, Communicare, Best Practice, etc.).
- Form Creator Access: Allows users to create/amend IT accounts and permissions for other users, but not approve them.
- User is a Delegate: This will grant the user the CEO's delegation to approve IT requests except for the granting of access to a user's emails and personal drive, which only a CEO can authorise. If this option is selected, the approval delegate for the form is automatically change to the CEO as only a CEO can approve delegation of their authority.
- Remove Account: When a user leaves the organisation it is highly recommended that something is done as soon as possible regarding their access. A decision needs to be made about what to do with their accounts and data. Three options are available:
  1. Active: If a profile had previously been disabled, this option will give the profile an active status in the user access from profile list.
  2. Disable: Emails and home drive are retained and the account is temporarily made inaccessible but can be reactivated if needed.
  3. Remove: Emails and home drive are retained but the account is deleted and cannot be reactivated.
  4. Delete: Emails, home drive and account are all deleted and cannot be recovered.

Step 4: Submit the request for approval

Once the form is complete select "Create" from any tab to submit the request for approval by the Delegate.

Delete user profile(s) from user list

If duplicate forms for a single user are identified, you can remove the redundant user access form(s) by clicking on the Delete button located at the bottom of the form.

You have to have a delegate from the delegate list selected for the delete button to become available.

Upon opting to delete a user access from, you will get the below warning.