Barts and The London NHS
NHS Trust

# How to Manage and Organise Shared Drives

## Guidance for Administrators

|  |  |
|---|---|
| | **Author:** C Redfern, E Donald |
| **Version Number:** 2.0 | **Date:** 10 Jan 2007 |

| Executive Summary | |
|---|---|
| **Aimed at** | • Administrators with responsibility for management of network shared drive folders and files |
| **Purpose** | • Save cost to the Trust by reducing amount of server space needed<br>• Ensure that Trust electronic records are managed, stored and retrieved efficiently when needed, retained for the appropriate period, and are disposed of in a timely appropriate manner.<br>• Ensure compliance with the Data Protection Act, Freedom of Information Act and Trust Records Retention Policy |
| **Benefits for Staff** | • Reduce time spent searching for information<br>• Increase sharing of information, reduce duplicate storage of same information<br>• Minimise duplication of information resources and effort |
| **Necessary skills** | In order to implement this guidance staff should have basic computer skills and be able to understand how to access folders via windows and save documents into these folders. |
| **Related Guidance** | • *How to Manage Email*<br>• *Where to Store and How to Share Electronic Documents* |

## CONTENTS

# 1. INTRODUCTION

**1.1** As part of our work we all create information, data, documents and records and we also need to share information with others.

The vast majority of electronic information created as part of the Trust's work should be stored on Directorate network drives, not on personal computers or personal drives (more information on this is available in the guidance document *Where to Store and How to Share Electronic Records* which is aimed at all staff).

However, if not managed, these drives can become out of control, unorganised, difficult to find information, and a repository for out of date and unnecessary information.

There are several good reasons for managing the shared drives.

**Reducing cost to the Trust (cost saving)** – If information is never deleted from the shared drive, the Trust will be forced to pay for more and more expensive server space. It is important to ensure that the Trust is not paying to preserve out-of-date or ephemeral information.

**Efficient retrieval of information (time saving)** – If the shared drive is structured logically and sensibly, folders have explanatory titles, and individual documents are named appropriately, this increases the ease by which information can be found. Relying solely on a “free text search” to find the correct document from tens of thousands of poorly named and poorly filed documents is not a practical solution.

**Reducing duplication and encouraging sharing of information** - A well managed shared drive encourages the sharing of information within Departments and teams, and helps to move away from individual filing systems in which many versions of the same documents are kept by individual members of staff. It also reduces the need to email documents since departments can access the document on the shared drive.

# 2. RESPONSIBILITES OF ADMINISTRATORS

Each Directorate shared drive should have an administrator, and each main “high level” folder should have a nominated individual to manage the contents of that folder. Whilst all individual staff are responsible for managing and filing the records they create, it is important that there is overall control of the folders to avoid chaos and confusion.

The administrator's responsibilities include:

- Granting access / manage security permissions
- Maintaining logical, controlled folder structure
- Ensure names of folders and documents comply with Trust naming conventions
- Encourage regular deletion of out of date, duplicate or unnecessary information.

- Manage the archiving of “closed” folders and files
- Liaising with ICT where appropriate

All staff should understand the folders which are relevant to their work, understand which ones they should use, and what sort of information should be stored there. All new staff who need to use the shared drive must be given an introduction to it by their line manager (or designated colleague) as part of their induction. More information for staff is available in the guidance document *Where to Store and How to Share Electronic Records*).

## 3. FOLDER STRUCTURE, NAMING AND TITLING

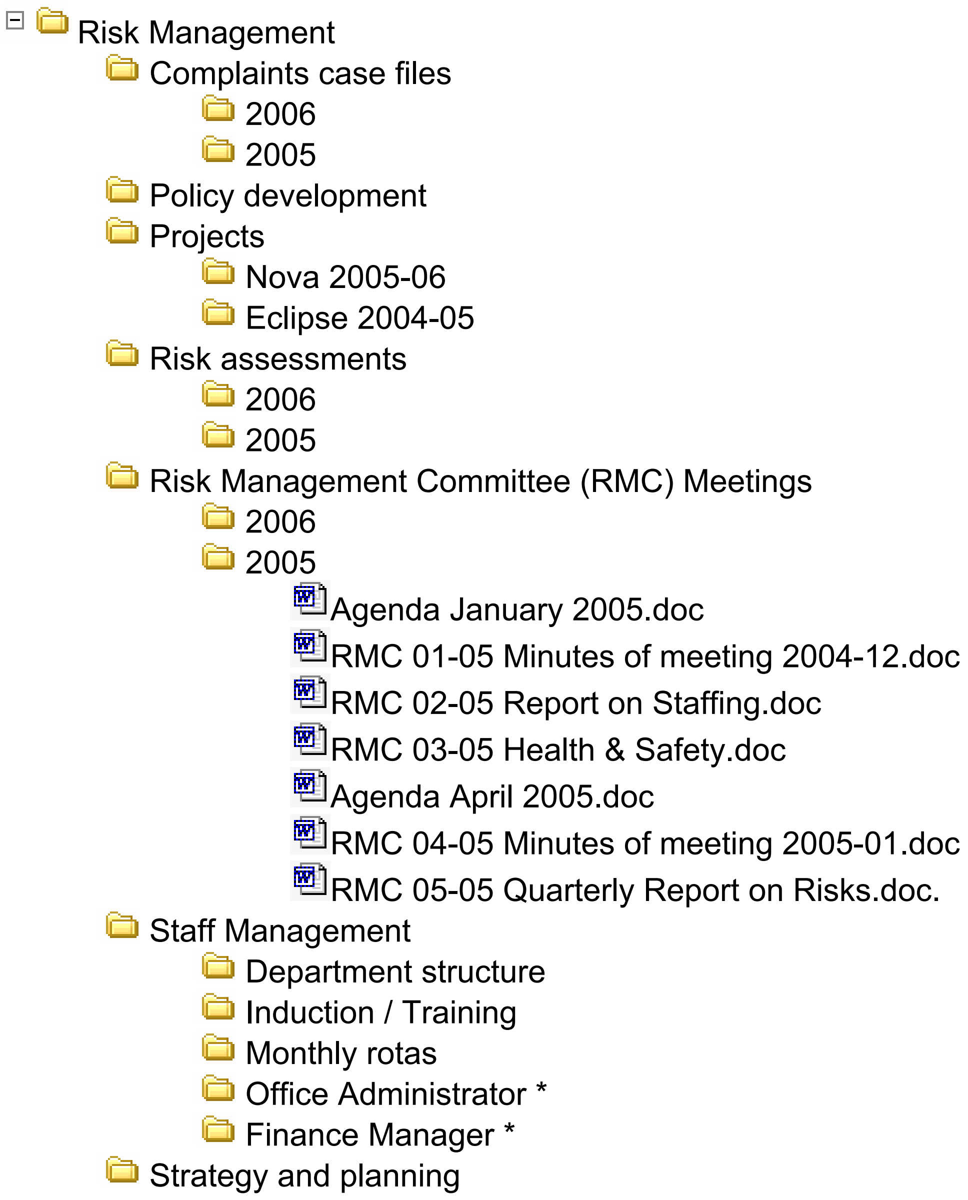
### 3.1 Key Principles

- Organise folders according to the **functions** / **activities** of the Directorate / Department, not individual members of staff. Department structures, team names, and individuals may change but functions and work activities will remain the same, or similar.
- **Keep it simple**: creating a complex folder structure causes confusion and problems in the long-run. Microsoft limits a path length to a file to 256 letters (this sounds a lot, but having a complex filing structure can exceed this limit).
- Sub-folders can exist in each folder, further categorising the records produced as part of the work activity. It is recommended to create **sub-folders for each year**, to avoid the folder becoming too large. This will also assist with identifying information which can be deleted in future.
- Records should be stored according to function/activity or subject, *not* file format. For example, store spreadsheets in the relevant subject folder, *not* separately in a folder called “Spreadsheets”
- All folder and file names must be relevant and easily understandable to all members of staff, including new staff.
- Names should be self-explanatory and meaningful: do not use “general” or “misc”
- Name documents consistently and logically.
- **Abbreviations** should be avoided but if used, should be expanded in the main folder title.
- Where lots of routine information is saved, create sub-folders for each year to help organise the records.
- All documents should be saved within a named folder. Avoid saving documents in the top level folders as they become lost – this is like putting loose papers into a filing cabinet instead of putting them into a file first.

All staff should be informed how to appropriately name folders and documents. A short guidance document, *Naming Conventions for Folder and Documents* is available on the Records Management intranet site, under Guidance. It is also included as an Appendix in the guidance *Where to Store and How To Share Electronic Records* which is aimed at all staff who use the shared drives.

To create new top-level folders, contact ICT. Sub-folders can be created by those who have been given “Modify” access to the folder.

## 3.2 Example 1 - a section of a well structured shared drive



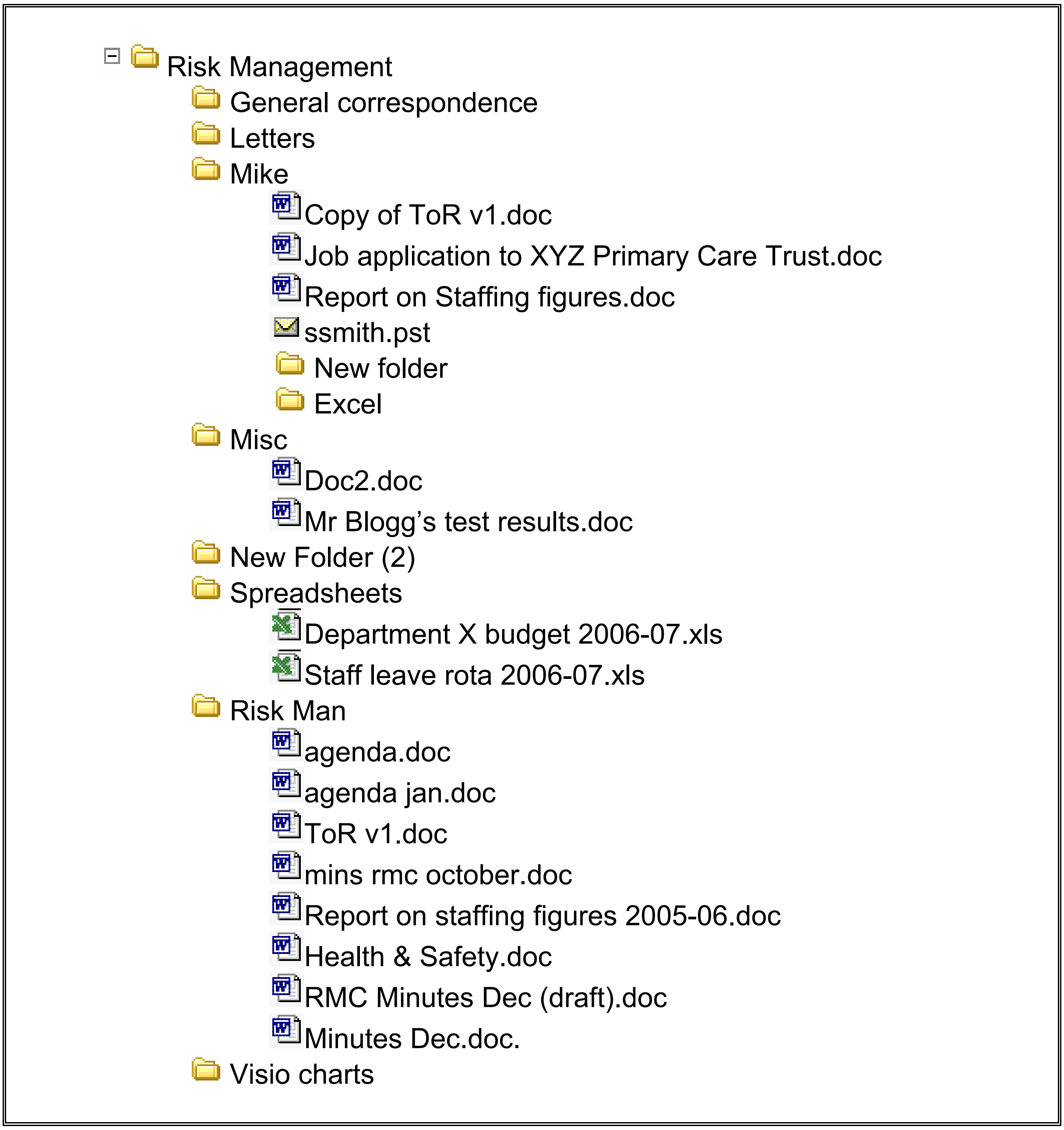
- Risk Management
  - Complaints case files
    - 2006
    - 2005
  - Policy development
  - Projects
    - Nova 2005-06
    - Eclipse 2004-05
  - Risk assessments
    - 2006
    - 2005
  - Risk Management Committee (RMC) Meetings
    - 2006
    - 2005
      - Agenda January 2005.doc
      - RMC 01-05 Minutes of meeting 2004-12.doc
      - RMC 02-05 Report on Staffing.doc
      - RMC 03-05 Health & Safety.doc
      - Agenda April 2005.doc
      - RMC 04-05 Minutes of meeting 2005-01.doc
      - RMC 05-05 Quarterly Report on Risks.doc.
  - Staff Management
    - Department structure
    - Induction / Training
    - Monthly rotas
    - Office Administrator *
    - Finance Manager *
  - Strategy and planning

** n.b. these files would contain job descriptions / generic job role information, not personal information about the individual*

**Good practice demonstrated:**

- Folders structured by activity / function
- Sub-folders structured by year, ensuring folders do not become too unwieldy.
- Clear naming: descriptions are self-explanatory
- No duplication: clear division of folders

### 3.3 Example 2 - a poorly managed shared drive



- Risk Management
  - General correspondence
  - Letters
  - Mike
    - Copy of ToR v1.doc
    - Job application to XYZ Primary Care Trust.doc
    - Report on Staffing figures.doc
    - ssmith.pst
    - New folder
    - Excel
  - Misc
    - Doc2.doc
    - Mr Blogg's test results.doc
  - New Folder (2)
  - Spreadsheets
    - Department X budget 2006-07.xls
    - Staff leave rota 2006-07.xls
  - Risk Man
    - agenda.doc
    - agenda jan.doc
    - ToR v1.doc
    - mins rmc october.doc
    - Report on staffing figures 2005-06.doc
    - Health & Safety.doc
    - RMC Minutes Dec (draft).doc
    - Minutes Dec.doc.
  - Visio charts

**Bad practice shown:**

- ○ Poor naming of folders and documents: no way of identifying contents
- ○ Patient information accessible to others: breach of patient confidentiality
- ○ Documents stored by type (format) rather than content: not logical – difficult to locate relevant information together
- ○ Personal information of staff accessible to others: breach of staff confidentiality
- ○ Personal names used in folders / personal filing structure being used: person could leave the Trust / Difficult for others to understand filing system or locate important information

  - Use of abbreviations: means something now but meetings and teams change names very quickly – meaning is forgotten over time
  - Personal use of Trust systems: unprofessional / against Trust Policy
  - Duplication of information: unnecessary storage costs on server; not clear which is the master version
  - Poor organisation of minutes: not clear which papers relate to which meeting; difficult to locate information; no indication of whether full set of minutes exist; not clear which version of minutes is the 'approved' or official version

## 4. ACCESS AND SECURITY

### 4.1 Key Principles

- Access to folders is granted to groups or teams rather than by individual members of staff. Individual members of staff are added to the relevant "Team Group", (which is also an email contact list). The access and security privileges are then applied to the group as a whole.
- The "Team Groups" are granted access to the relevant top level folders on the drive. The access is 'inherited' down through the sub-folders.
- There may be several Team Groups in a single Directorate.
- When a member of staff leaves or joins the Trust the relevant Team Group is amended.
- Ensure folders which must contain patient information have correct levels of security / check permissions and update ICT if someone leaves the Trust.
- Personal information about individual members of staff should be kept on the line manager's H: drive (their personal drive) rather than being put onto the shared drive.

### 4.2 Setting up the Team Groups

To set up the Team Groups, contact ICT. Each of the Team Groups should have a named administrator (preferably the same person who administrates the folder structure) to ensure that the team group is kept up to date. The administrator is responsible for adding and removing team members.

### 4.3 Levels of access

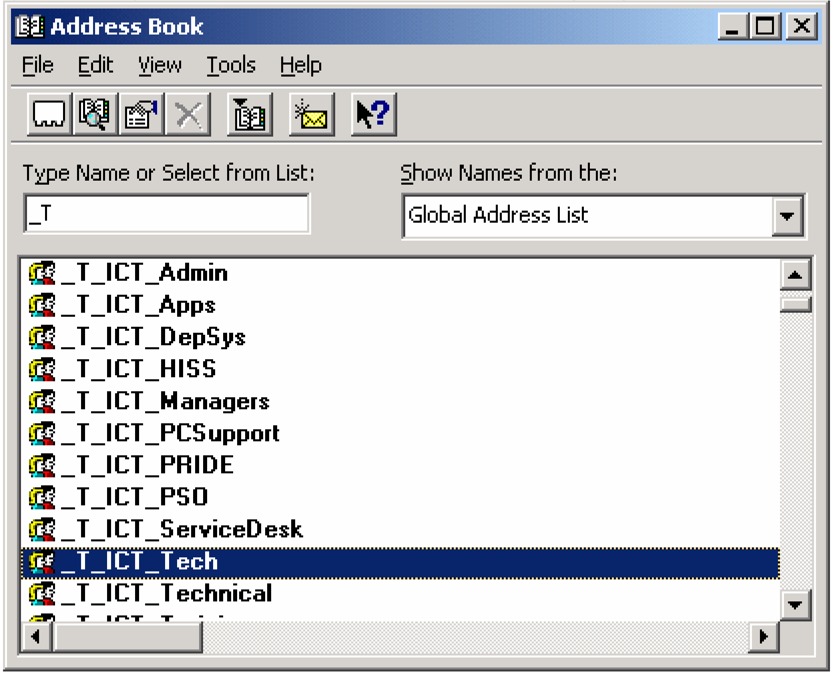
The Team Group can be given a different level of access depending on the level required. For example, one team group could have "modify" access over their own folder but "read and execute" access to the folder of another team. The different levels of access are:

| Level of Access | What you can do | Suitable For |
|---|---|---|
| Full Control | Allows the administrator to delete top level folders and manage access / security permissions. | Administrators only. |

| | | |
|---|---|---|
| Modify | Create documents and folders, read, edit, and delete documents, and delete sub-folders which you created. | Staff who need to add documents to the folder. |
| Read & Execute | Read the files and run a programme (you usually need to be able to run a programme, e.g. Word, in order to read the files). | Staff who need to read but not add to the folder. |
| List Folder Contents | Not recommended | |
| Read | Not recommended - Use Read & Execute instead. | |
| Write | Not recommended - Use Modify instead | |

## 4.4 Adding and removing team members

1. If you are a designated manager for the team group, you have permission to add and remove members from the group. To do this open up Microsoft Outlook and go to the Address book.
2. In the **Type Name or Select from List** box add the name for your group. This will save you having to scroll down the entire list. The group name will be in the form of _T_Project_Team or _T_Directorate_Team, as in the example below of _T_ICT_Tech.
3. When you find your team in the address list highlight it and double click.

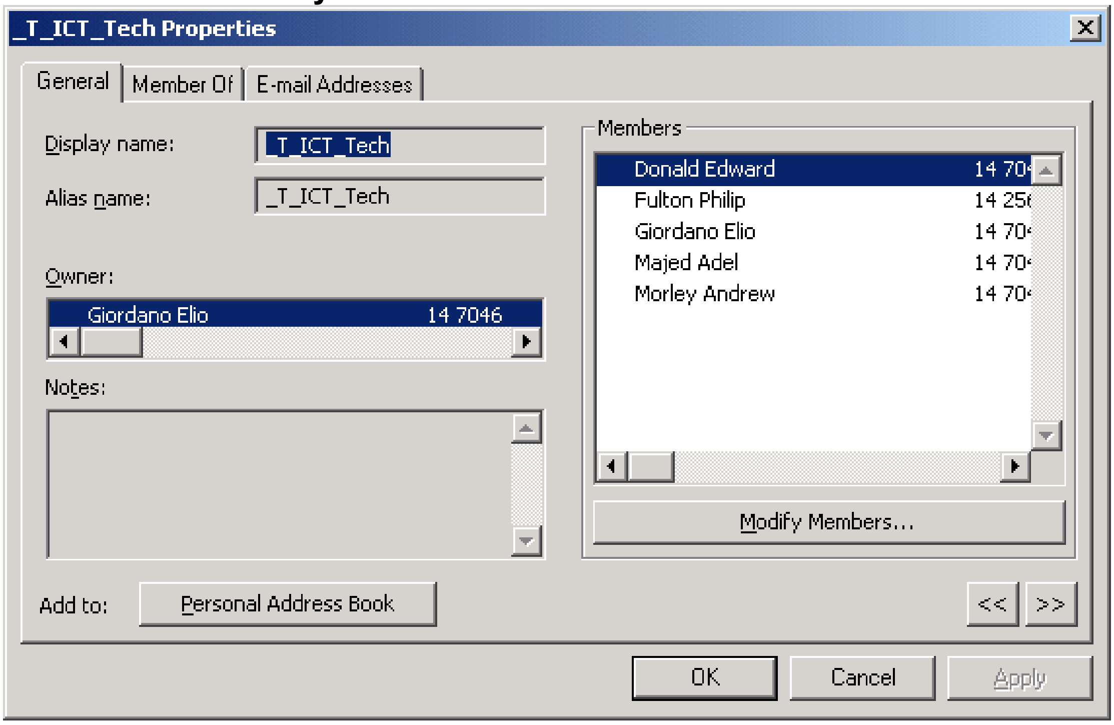


Type Name or Select from List: _T

Show Names from the: Global Address List

- _T_ICT_Admin
- _T_ICT_Apps
- _T_ICT_DepSys
- _T_ICT_HISS
- _T_ICT_Managers
- _T_ICT_PCSupport
- _T_ICT_PRIDE
- _T_ICT_PSO
- _T_ICT_ServiceDesk
- _T_ICT_Tech
- _T_ICT_Technical

4. It should now display the properties for your team. If you are the Owner then you can add or remove members to the team group. To change group membership click on the **Modify Members** button.



Display name: _T_ICT_Tech

Alias name: _T_ICT_Tech

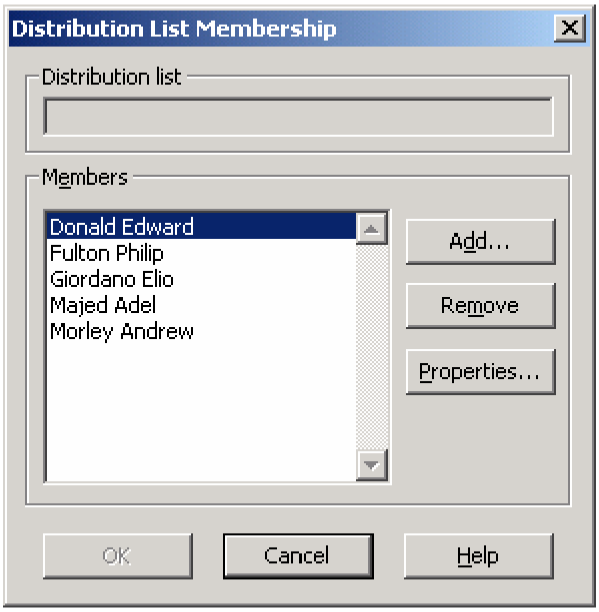
Owner:

| | |
|---|---|
| Giordano Elio | 14 7046 |

Members

| | |
|---|---|
| Donald Edward | 14 70 |
| Fulton Philip | 14 25 |
| Giordano Elio | 14 70 |
| Majed Adel | 14 70 |
| Morley Andrew | 14 70 |

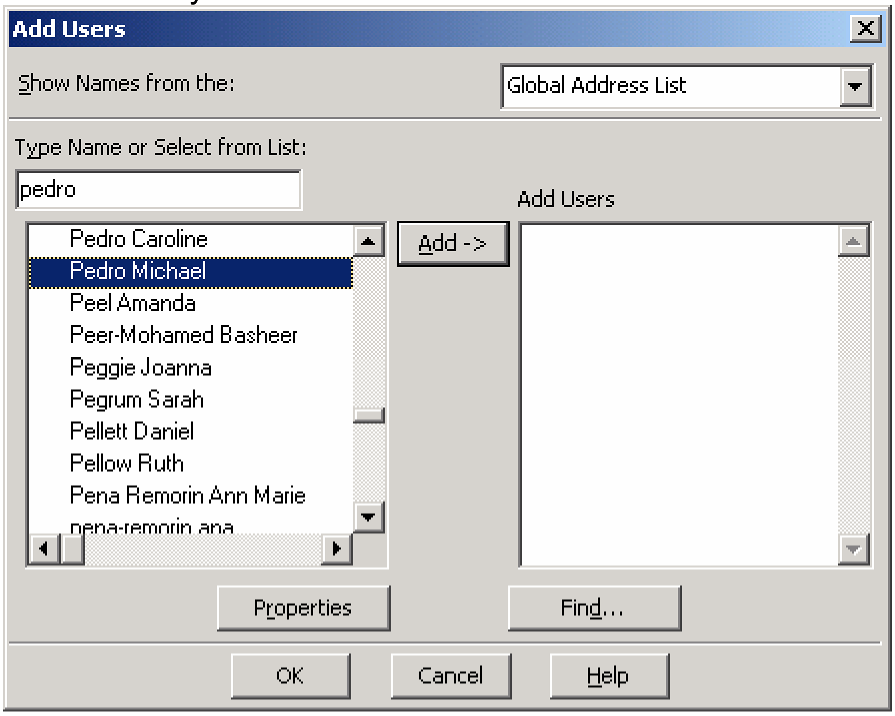
5. If you wish to remove a member from your team (for example because that member has left the Trust or your team) then highlight their name and click on the **Remove** button and then **OK**. This is all that is required. If, however, you need to add someone to the team group click on the **Add** button and follow the instructions below



Members

- Donald Edward
- Fulton Philip
- Giordano Elio
- Majed Adel
- Morley Andrew

6. A new window **Add Users** will appear. Again in the **Type Name or Select from List box**, start typing the surname of the user you wish to add. The user will of course need to have had an email account set up already. You may discover that there are several users with similar names on the list. If you are in any doubt which is the correct one then highlight the user you believe to be correct and click on the **Properties** button. If the team folder is on the I drive then you can add members from any directorate. If the team folder is on the Q drive only add members of your own directorate.



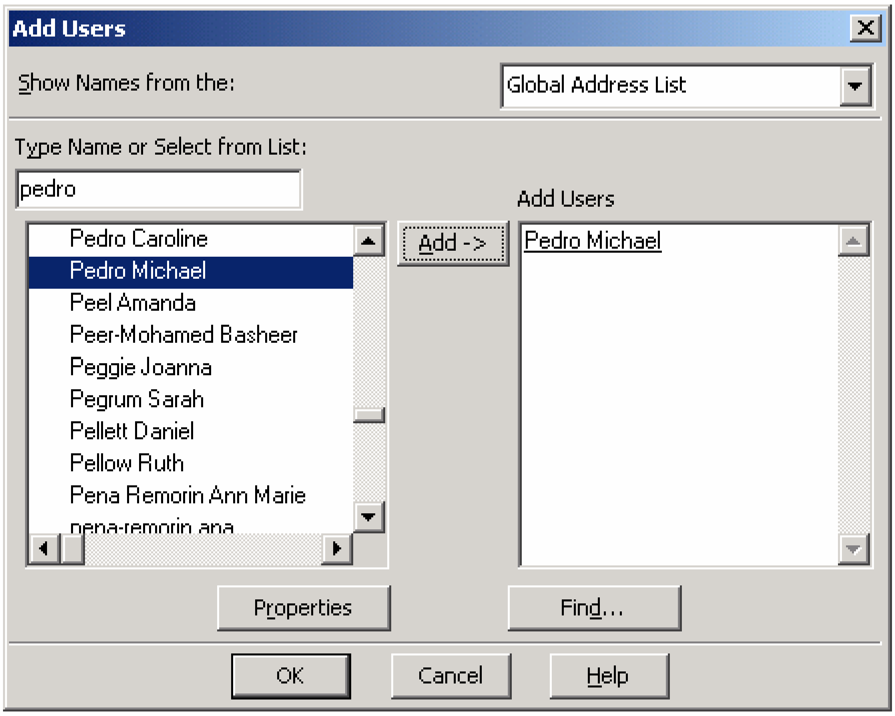
Show Names from the: Global Address List

Type Name or Select from List: pedro

Pedro Caroline
Pedro Michael
Peel Amanda
Peer-Mohamed Basheer
Peggie Joanna
Pegrum Sarah
Pellett Daniel
Pellow Ruth
Pena Remorin Ann Marie
pena-remorin ana

7. This will display information about that individual including their job title, office and department. This should be enough to decide if the user is from your team. Repeat the process if it is not the right user.

8. Once you are satisfied you have the correct user then click on the **Add** button and OK. Please note: Unfortunately because this process gives a user rights to a group for email and folder permissions you may not be able to add several members to the group simultaneously.



Add Users

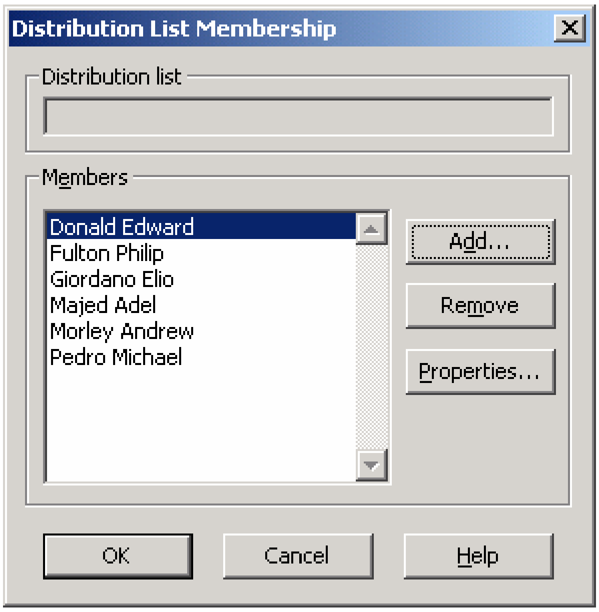
Show Names from the: Global Address List

Type Name or Select from List: pedro

Pedro Caroline
Pedro Michael
Peel Amanda
Peer-Mohamed Basheer
Peggie Joanna
Pegrum Sarah
Pellett Daniel
Pellow Ruth
Pena Remorin Ann Marie
pena-remorin ana

Add Users: Pedro Michael

9. If you have no more users to add click on OK to close the screen



Distribution List Membership

Distribution list

Members

Donald Edward
Fulton Philip
Giordano Elio
Majed Adel
Morley Andrew
Pedro Michael

10. Click on OK again to leave the Team properties.

## 5. MAINTENANCE AND RECORDS MANAGEMENT

As time goes by, the amount of data stored will increase greatly and the amount of server space taken up by the drive will grow.

A regular (e.g. yearly) spring clean will stop your file structure becoming too unwieldy. Deleting data that is no longer required is one way of keeping your folder structure manageable.

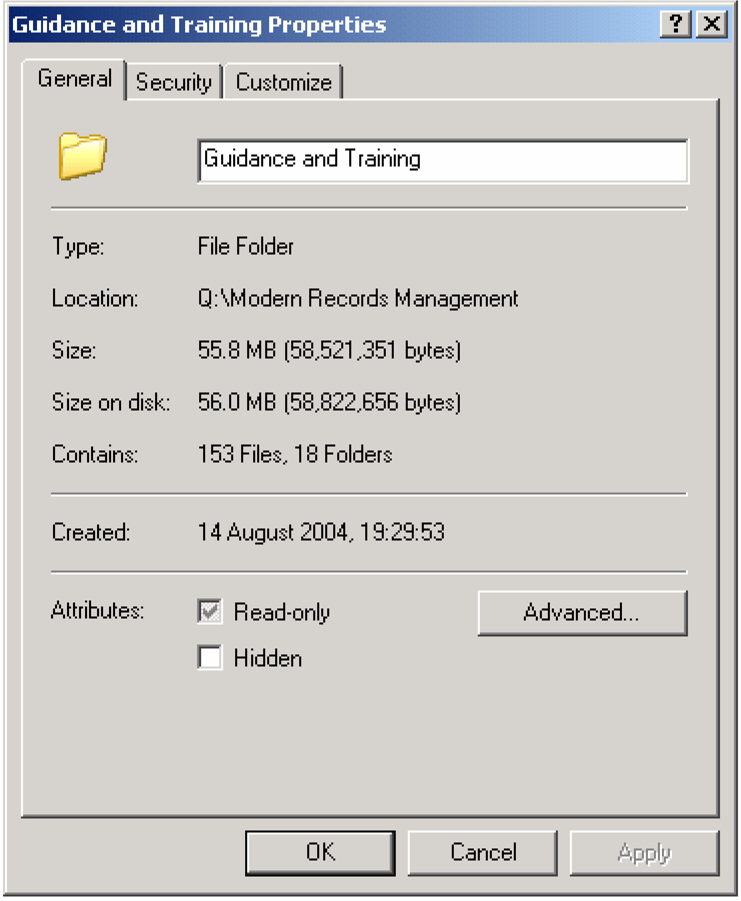
Staff should be encouraged to undertake a review of their records on the drive. The following guidance is to assist staff in undertaking this review. If you are spring cleaning the folders make sure all relevant staff are informed first.

**When can records be deleted?**

The Trust Records Retention and Disposal Policy gives detail of when records can be destroyed. If the shared drive contains information which is not described in the Policy, contact the Modern Records Manager for advice. All records should be destroyed in accordance with this policy.

**To find out the size and number of items in a folder**

Right click on the folder and choose properties. This will bring up a box showing the size in kilobytes, the total number of items in the folder and sub-folders, and the number of folders within. This can help to identify which folders are the largest and prioritise which require attention.



Guidance and Training Properties

Guidance and Training

Type: File Folder

Location: Q:\Modern Records Management

Size: 55.8 MB (58,521,351 bytes)

Size on disk: 56.0 MB (58,822,656 bytes)

Contains: 153 Files, 18 Folders

Created: 14 August 2004, 19:29:53

Attributes: ☑ Read-only ☐ Hidden

### Identify the largest items

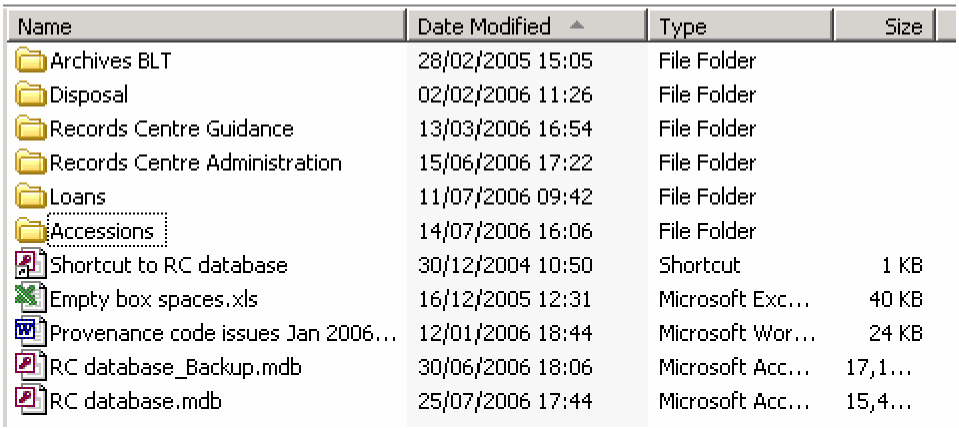
Identifying the largest items in the drive or a folder, and seeing if any of these can be deleted, can be a quick way of freeing up space on the system. To do this, select the drive or folder, right-click and choose search. In the search box, choose to search for items by **size** and type in the amount of KB (e.g. 10,000). The search results can be ordered by size, by clicking on the **size** tab, to immediately identify the largest items on the drive. Any items which can deleted can be deleted from the search window.

Common large items include:

- *Bitmap images (.bmp)* - These should be saved as .Jpgs and then deleted.
- *Powerpoint Presentations* - Powerpoint presentations can become quite large especially if they contain pictures. You can compress the pictures to reduce the size of the Powerpoint file, but the quality of image will not degrade. To do this: In powerpoint, ensure you have the “Picture” toolbar visible, by going to View – Toolbars – and choosing Picture. You will see some new buttons appear. There is a button which looks like four small arrow pointing inwards towards a picture. Click on this to compress the images and remember to save the presentation when you leave. This also makes the presentation faster to load.
- *Access databases* – Ensure that the database is not a duplicate copy and check whether it is out of date or can be deleted.

### Identify old / out-of-date items

To do this, select the drive or folder, right-click and choose search. In the search box, choose to search for items by **date** and search for files modified between certain dates (e.g. between 1980 and 1990). The search results can be ordered by date, by clicking on the **date modified** tab, to immediately identify the oldest items on the drive. Items which have not been modified for a long time may be likely candidates for deletion. Any items which can deleted can be deleted from the search window.



| Name | Date Modified ▲ | Type | Size |
|---|---|---|---|
| Archives BLT | 28/02/2005 15:05 | File Folder | |
| Disposal | 02/02/2006 11:26 | File Folder | |
| Records Centre Guidance | 13/03/2006 16:54 | File Folder | |
| Records Centre Administration | 15/06/2006 17:22 | File Folder | |
| Loans | 11/07/2006 09:42 | File Folder | |
| Accessions | 14/07/2006 16:06 | File Folder | |
| Shortcut to RC database | 30/12/2004 10:50 | Shortcut | 1 KB |
| Empty box spaces.xls | 16/12/2005 12:31 | Microsoft Exc... | 40 KB |
| Provenance code issues Jan 2006... | 12/01/2006 18:44 | Microsoft Wor... | 24 KB |
| RC database_Backup.mdb | 30/06/2006 18:06 | Microsoft Acc... | 17,1... |
| RC database.mdb | 25/07/2006 17:44 | Microsoft Acc... | 15,4... |

### Reviewing the folders

Another useful exercise is to browse through the main folders in turn. This can help to identify information which was once created but has been forgotten and can be removed.

## 6. "All_Trust" folders

**6.1** There are numerous projects/meetings which involves people working in more than one directorate. If this is the case, a folder can be created in the "All Trust" section of the I: Drive for the storage of these records. Folders suitable for this include:

- Records or documents which need to be regularly shared and accessed by members of more than one Directorate.
- Ongoing work / projects or meetings involving staff from more than one Directorate.
- Meeting papers where members are from more than one Directorate.

To discuss setting up an "All Trust" folder, contact ICT. The folder should be managed in the same way as any other folder on a shared drive and an individual should be given responsibility for its management and maintenance.

## 7. RESOURCES

### 7.1 Guidance documents

Available at http://bltintranet/A-Z/Recordsmanagement/recordsmanagement.aspx

| **Guidance Document** | **Purpose / Aimed at** |
|---|---|
| *Trust Records Retention and Disposal Policy.* | Trust Policy explaining how long to keep records |
| *Where to Store and How to Share Electronic Records* | Aimed at all staff who create electronic records and use the H: drive or shared drives |
| *Naming Conventions for Folders and Documents* | Aimed at all staff who create electronic records and use the H: drive or shared drives |
| *How to Manage Email* | This is guidance for all staff who use email; it contains:<br>• handy tips and exercises for reducing the amount of emails you hold,<br>• finding relevant emails quickly,<br>• using Outlook tools to manage your emails,<br>• ensuring that important emails are captured as records, and<br>• helping to comply with legislation and Trust Policy. |
| *Use of Trust Email Policy* | Trust Policy covering the appropriate use of email |

## 7.2 Contacts

| Contact | Expertise |
|---|---|
| Catherine Redfern, Modern Records Manager | Records Management<br>Retention and Disposal of Records<br>Freedom of Information<br>Folder structures<br>Naming and titling of documents |
| Nicola Gould, Information Governance Manager | Information Governance<br>Data Protection<br>Freedom of Information<br>Information Security |
| ICT Helpdesk | Access and Security to electronic folders<br>Setting up Team Groups<br>Setting up new top-level folders |