Protect and **survive**

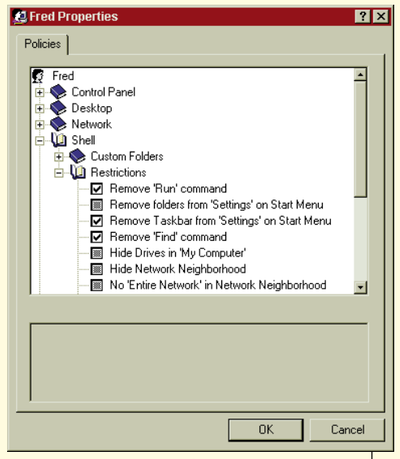
Tim Nott **tightens up security in Windows 95 without the aid of deadlocks and dobermans.**

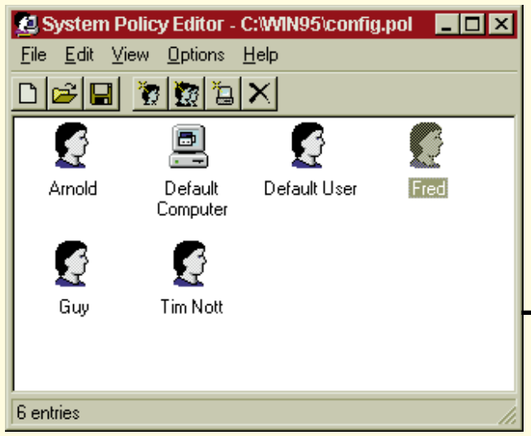
There must be many readers who have the responsibility for more than one user on the same standalone PC. Whether you're an employer, an administrator, a parent, or like reader Robin Malton, a teacher, there's the perennial problem of preventing the user from "customising" the settings in ways that screw things up for other users.

As Robin states: "*Most IT teachers have developed strategies for locking their pupils out of areas of Windows 3.1. Now we have got to start all over again with Windows 95. We are about to buy up to 20 standalone machines and the thought of all the chaos which will be created, intentionally or otherwise, by unrestrained use of Settings for Task Bar and Control Panel, let alone the freedom of My Computer, is causing grey hairs.*"

Windows 3.1 has some fairly minimal locks; notably the restrictions that can be made to Program Manager and Control Panel by editing the .INI files. Windows 95 is no Fort Knox (for real security, you'd use NT Server) but it does go a fair bit further.

First, a brief word on User Profiles and System Policies. User Profiles are basically those bits of the Registry that are stored in USER.DAT. On a network, these can be used in two ways. Firstly, System Policies can be set up to give mandatory profiles to users (or groups of users), with restrictions to stop them altering various aspects of their system. The obvious advantages of this are the savings in training and support costs. Secondly, profiles can be made "portable", which means roving users can log on from anywhere on the network and fire up their own desktop. In these cases, policies and profiles are stored on the server.





Above
Restricting Fred's access…

Left
Defining different users in the System Policy Editor

Fortunately, networks are not my brief. However, the same tools can be used on a standalone PC to give different users various settings or levels of access. You might, for example, share a PC with a colleague who works a different shift, but still want to keep your own desktop settings. Or you might, like Robin Malton, want to prevent reckless or mischievous meddling.

A matter of policy

It's a lot more complicated and confusing than the pre-95 editing of plain-text .INI files and, as you've probably already guessed, involves the Registry. The usual warnings about backing up USER.DAT and SYSTEM.DAT apply here in spades. It's extremely easy to foul things up, lock yourself out of the system and seriously damage your mental health. It's also appallingly documented, but after consulting the Windows 95 resource kit, the Microsoft Technet, with a bit of inspired guesswork and a lot of trial and error, I think I've just about got the drop on it.

The good news is that Microsoft has provided a specific tool for the job, the System Policy editor. This is on the Windows 95 CD. Use Control Panel/Add-Remove/Windows Setup/Have Disk then browse the CD to

```
\ADMIN\APPTOOLS\POLEDIT\
```

to install it. As the helpfile isn't much help, have a look for

```
\ADMIN\RESKIT\HELPFILE\WIN95RK.HLP
```

as well. This is the Windows 95 resource kit, which contains a mine of useful information in a helpfile. If you installed from floppies, or had Windows 95 pre-installed on a PC, then the files are available from Microsoft (see *PCW Contacts*, page 250).

Having installed the Policy Editor, the next step is to enable User Profiles. From Control Panel/Passwords, select "Users can customise…". Make sure the two options below are also ticked, then restart the computer. You'll be prompted for a user name and password. This user is going to be *you* — the System Administrator and Master of the Universe — so choose wisely. You'll be asked if you want to retain your settings between sessions. You do.

You'll find that things have changed somewhat. In the Windows folder, you'll find a new folder called Profiles. Inside this will be a single folder corresponding to your user name. Inside that will be your own personal registry files: USER.DAT and USER.DA0 (the backup), and three other personal folders: Desktop, Briefcase and Recent. You might also find that some of the files, folders and shortcuts that were on the desktop have disappeared. Don't panic, they can still be found in the Windows\Desktop folder. You'll also find that the close-down dialogue has sprouted an extra option: "Close all programs and log on as a different user".

The installation of Poledit should have copied a file called ADMIN.ADM to the WINDOWS\INF folder. If not, or if you installed Poledit by hand, you'll have to copy this from the CD. Once POLEDIT is installed and running you may get prompted to choose a template: if so, browse to WINDOWS\INF to find ADMIN.ADM; if not, check that this file is the one cited in the "Options/Template" menu. If you can't find the INF folder, then select "View/Options/View" from any open folder and tick "Show all files".

Open the "File" menu and choose "Load Registry". You'll see two items appear in the main window: "Local User" and "Local Computer". Double-clicking on either of these produces a new window that looks rather like a Helpfile contents with an expanding tree of book icons.

Network?... What network?

Now it starts to get hairy, as even the Resource Kit leaves you on your own. The correlation between system policies and user profiles is a nebulous thing and, at least on a standalone PC, gives the impression that the groups of programmers responsible didn't like each other very much.

The first thing to do is alert the Registry to the fact that not only are there different users, but that system policies are in effect. In other words, Windows has to look for a policy file on startup. Open "Local Computer" and double-click the "Networks" book. Yes, I know you're not on a network, but remember I mentioned the words "complicated" and "confusing" earlier. Double-click the "Update" book, then tick "Remote Update". In the panel below, choose "Manual (use specific path)" in the "Update Mode" box and type in a path below that. Using the defaults, this would be

```
C:\WINDOWS\CONFIG.POL.
```

OK the dialogue, then save and close the Registry.

Now open a new file in the Policy Editor. Again you'll see the same items, but this time you'll be able to add new users from the "Edit" menu. Add one with exactly the same name you logged in with. Click on yourself and you'll see five "books": Control Panel, Desktop, Network, Shell and System. These all expand into a series of check boxes which can be in one of three states. Ticked means the policy is in force or, if it isn't, will be put into force next time that user logs on with the Registry amended to suit. Clear means the policy isn't in force, or will be removed from the Registry at the next log-on. Greyed means that the status quo will be preserved. Nothing will be added to, or removed from, the Registry.

In general, it's better to grey than to clear. For a start, clearing can remove settings you may not want removed. Secondly, as greyed settings are ignored, processing the registry is much faster. Some settings, such as the "Update" in the last paragraph, have an extra panel below.

To get the hang of this, experiment with your own ID and something harmless. All user policies should be grey to start with, so go to "Desktop/Wallpaper", tick the box and choose a wallpaper file from the list. Obviously, choose something different from the current one. Save the Policy file with the name you specified earlier (C:\WINDOWS\CONFIG.POL) and close down Windows. If you log on as yourself again, you'll see your wallpaper has changed to that specified in the policy. You can change it back, assuming you haven't restricted Control Panel access, but only on a per-session basis. Clearing the box, in this case, means you'll always start without any wallpaper. Greying the box means that the Control Panel wallpaper settings function as normal and are saved between sessions.

Once you've got the hang of this, you can begin restricting the Default User. All new users will be based on these settings. If you expand the tree, you'll see that the Control Panel section can restrict various levels of access to the Display, Network, Passwords, Printers and System. All are adequately explained in the sub-options so I won't go into much more detail. You'd probably want to enable all the restrictions in the System section, for instance, and also at least keep users away from the Display/Settings page. Somewhat strangely, you can't protect other sections, so users are free to screw up their fonts, multimedia and other settings.

School uniform

The Desktop section lets you set mandatory wallpaper and colour schemes, if you're into the "regulation issue" look. The Network section, which is about file and printer sharing, needn't concern us. Moving on, the Shell section gets more interesting. First, you can decide whether users can

have their own custom folders for the Start menu and Desktop. In a classroom situation you might not want this, but two people sharing a PC probably would.

The next bit is where it gets interesting for wannabe System Stalins. Under Shell/Restrictions is plenty of privilege waiting to be taken away. You can disable the "Run" and "Find" and "Settings" commands from the Start Menu, remove drives from "My Computer" or even everything from the desktop. There's a "Don't save settings" option which is extremely useful as it means that users can't leave a mess of open folders for the next person; and finally, there's an option to disable the Shut Down command. This latter is a very bad idea as the only way to exit Windows is by resetting the computer. This, as many Windows 95 users have found to their cost, is an open invitation to the gremlins of chaos to invade the machine.

Under the next "System" section you can disable both normal and single-mode DOS sessions as well as Registry editing tools. It is rather misleading as it doesn't disable Poledit, only Regedit, so you might want to make sure the former isn't left on the hard disk of the PC. The final, and most restrictive, setting is to "Only run allowed Windows applications". The bad news here is that you have to type in a list of each application by hand; you can't browse or select. However, having done this once you can, of course, copy the policy file across a classroom full of machines.

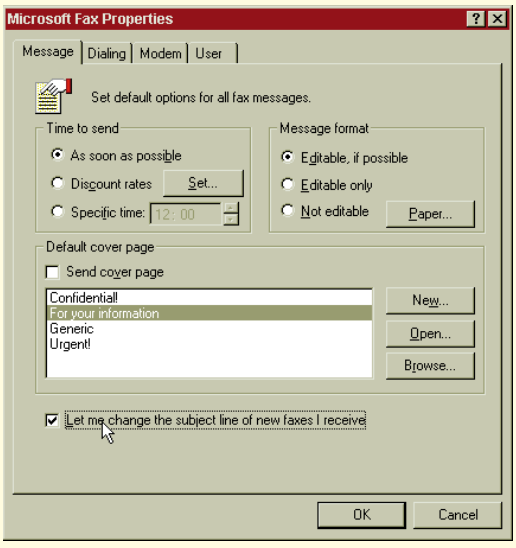
Having set up restrictions for the Default User, do check that you haven't inadvertently restricted yourself. I have a strong suspicion that some settings "migrate" but I haven't yet caught them in the act. Save the policy file, exit Poledit and exit Windows. You should now find that when any new users log in with a new name and a password, they will inherit the default user restrictions.

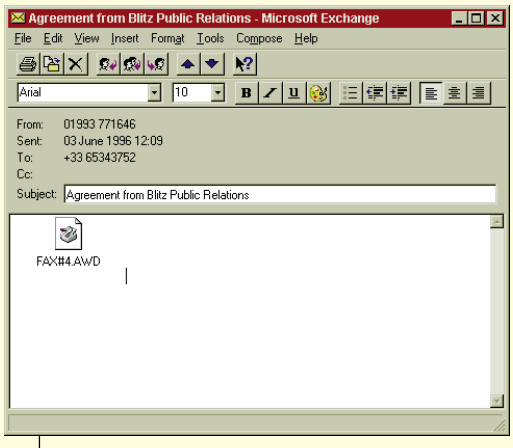
Plugging the hole

With multiple users enabled, as I said earlier, you get a password prompt on logging in, with the default name of the last user. Although you'd obviously want a password for the system administrator, passwords are not obligatory. You could have "Class 5A" as a user with a blank password. There is, however, just one teeny-weeny snagette. If you hit the "Cancel" button, everything reverts to where we came in. The desktop goes back to how it was before multiple users were enabled, and all restrictions are lifted.

If you log back on as yourself, run Regedit and open HKEY_USERS, you'll see two branches: one with your name and another named .Default. The latter retains the original settings and is used when the "Cancel" button is pressed during log-on. So just do this: restart Windows, hit "Cancel" and run Regedit again. You'll see just .Default in HKEY_USERS. Close Regedit, run Poledit and open the Registry. Now apply the same restrictions to the Registry as you did to the default user in CONFIG.POL. You'll then find the Cancel button leads to the same restricted environment as the default user log-in. If you want to restrict all users to the same degree, you can skip all the above except for the previous paragraph. Bear in mind, however, that you want to leave yourself a way in to the system.

It's still by no means perfect. There are more holes in it than in the Swiss Emmental cheese mountain. There's no way to password-protect folders or partitions, which means that as long as users can open one folder, they have access to the entire PC. Even with all restrictions in place and just Notepad.exe in the list of permitted programs, it's a trivial matter to open Explorer from the File/Open dialogue.





Top *Enabling this setting…*
…lets you give meaningful descriptions to incoming faxes **(above)**

Another big nuisance item is that anyone can create a new user ID and insist on having their settings saved, which can lead to a proliferation of unwanted individual folders, even though the Custom folders options are cleared for Default User.

A couple of further safeguards you might like to consider are setting BootKeys=0 in MSDOS.SYS so the user cannot use the function keys to stop Win95 loading at startup. You might also like to disable floppy disk-booting from the PC's CMOS settings, and password-protect the CMOS itself. This process will vary, so you'll need to consult the hardware manual.

What the fax?

And now for something completely different and far less brain-damaging. In July's column I had a good moan about Exchange, but recently I've actually managed to discover something I like.

Looking through the faxes in my Inbox I was struck by the fact that in the "From" column was the number of the caller. If the caller hadn't set their fax machine or software to give this information, then it stated "Unknown fax machine". The "Subject" field didn't actually tell me anything more. It either showed that this was a fax from the number in the adjoining column or, if this was unknown, simply "Fax".

Rather a waste of time and space I thought, until, browsing the Inbox menus, I came across the following well-buried secret. From the "Tools" menu, go to "Microsoft Fax Tools/Options". Or, if you prefer the scenic route, go "Tools/Options/Microsoft Fax" and click the "Properties" button. Either way, you get a four-page dialogue for "Microsoft Fax Properties". And there, on the "Message" page, is a tick box for "Let me change the subject line of new faxes I receive". Which says it all really. Now, when you double-click on a fax in the Inbox, instead of going straight to the viewer, you're in the fax editing window with the fax file shown as an icon. Double-clicking on the icon launches the viewer, but the bit I like is that you can now alter the "Subject" field to read something sensible and informative.

PCW Contacts

Tim Nott can be contacted either by post c/o *PCW* or by email at **timn@cix.compulink.co.uk**
No hawkers, circulars or binary attachments, please.

Microsoft 0345 002000; www.microsoft.com