
The Computer Club At Willow Valley

The President's Pen by Sid Paskowitz

Inside this issue:

| | |
|---|----------|
| Coming Programs | 2 |
| Sysinternal's Process Explorer | 4 |
| Do This and Your SSD Will Last Much Longer | 5 |
| The Equipment Corner | 9 |
| The Mission | 9 |
| The Leadership | 9 |

Membership As of this writing, your Computer Club has 572 paid members including 369 who have signed up as Lifetime members. Please keep your email address current on Club records so we can send you important emails. *Those emails only go to Computer Club members for whom we have a good email address.* Let our Treasurer, Charlie Trumbo (chtrumbo@gmail.com), know if your email address has changed or if you don't get a future Newsletter. When I recently sent out an email advising Computer Club members about the closing of the Kendig Square Radio Shack and the significant price reductions that were available, 10 of those emails were returned as undeliverable to invalid email addresses. I did receive several responses from those who got the email and they told me how much they saved on the items there were looking to buy.

April Meeting My thanks to those of you who braved the terrible weather and attended the Information Central presentation at the April Computer Club meeting in the Cultural Center Theater. In light of the positive response to the presentation but the reduced number of attendees, we will be scheduling a repeat of the Information Central presentation. Watch the Weekly Insider for the time and date for that presentation in the Manor North Johnson Auditorium. Everyone is welcome to attend. If the presentation is well-received and Residents want the presentation to be repeated in other Community auditoriums, tell your Community Resident Life Manager.

Renaissance Classes We will be trying something new for the Summer Renaissance classes. Instead of the presenter developing a presentation of material based on what the presenter thinks might be of interest to the attendees, we will be contacting the class registrants and asking them to submit questions that they would like to have answered during the class. We will then set up a panel of presenters who are best able to answer those questions. We may also send an email to registrants and tell them what will be covered in the class based on the questions we receive. If this approach is successful, we will continue this type of class in future Renaissance publications.

Update Your Online Directory Something some Residents may not know: you can update or correct your own information in the Willow Valley on-line phone directory. Left-click on the Resident Directory tile on the Kiosk Home Page; then left click in the Phone Search box; then put your last name in the empty box to the left of the Search button; review the information displayed about you; and if you note something such as your email address that needs to be

(Continued on page 2)

Coming Programs

May 4

Peter Scott, Willow Valley Resident
Back to Some Computer Basics

June 1

Al Williams, Willow Valley Resident
The Dark Web

July and August

No Computer Club Meetings

*All programs are held
in the Theater at the
Cultural Center
on the 1st Thursday of
the month at 2:00 p.m.
unless otherwise noted.*

President

(Continued from page 1)

changed, left-click on the link *Click here to make a correction*. Fill in the information on the next screen and say what you want to be done in the Comments box. When you are satisfied you have clearly stated what you want done, left-click on the *Submit* button. In a day or so, check your information in the on-line directory to verify the desired change was made. When your email address is correct in the on-line phone directory, it can save you and other Residents a phone call when they want to send you an email. Please note that if you change your email address in the on-line directory, that does not update your email address in Computer Club records as discussed earlier. Many Residents have multiple email addresses and use them for different purposes, so if you want your email address changed in Computer Club records, you will need to notify Charlie Trumbo.

Scams, scams, scams... No one who calls you, emails you or displays a message or your computer or device can tell you your computer or device is infected or running poorly. They have to have been given access. If you haven't provided them with access, you are being scammed. Don't give them access. Hang up. Disconnect. Shut down. Also do not respond to emails that say your account is missing information or they were not able to deliver a package with something you did not order. Be skeptical. **Protect yourself.**

Some new, but not surprising, information about malicious software: Google found Android spyware in its app (application) store. **That spyware had been there for three years without being noticed.** Millions were potentially affected. This brings up an interesting point I would like to emphasize. The Computer Club tries to be selective in the PC software we recommend and those recommendations change over the years when we

(Continued on page 3)

President

(Continued from page 2)

find software we like better. For example, a number of years ago we recommended Zone Alarm as the preferred firewall and AVG as the preferred anti-virus software. Today we recommend the Windows firewall and Windows Defender, Windows Security Essentials, or Malwarebytes as the anti-virus software. There are other programs that perform similar functions but we have experienced good results with the programs we recommend. We suggest caution in loading programs that may pop up on your computer screen or might be listed when you do an Internet search for software that might address a problem you are having. The experience with the Google store demonstrates that being skeptical can have its virtues.

Windows 10 Plans Microsoft is still working hard to hit the one billion mark for Windows 10 users and two recent reports have indicated their moves in that direction. First, Microsoft plans to have two major upgrades to Windows 10 and Office annually, probably in March and September. Second, reports have been received that some Windows 7 and Windows 8.1 computers have been successfully activated with Windows 10 using old license keys. I am not recommending non-techies try to do this. I just want readers to be aware this may be possible if you want to upgrade to Windows 10 without needing to buy a new computer.

Please Use Recommended Software PC owners are reminded that they can receive the best help if they use software that is familiar to other Residents who volunteer to provide technical assistance. Recommended applications are CCleaner, Malwarebytes, Defraggler and Windows Defender (or Windows Security Essentials). We recognize there are alternatives; however, problems are more quickly diagnosed and repaired when the applications running on the PC are familiar to the helper.

Classes We know we need more classes on computer-related topics and we are looking for instructors who can teach those classes. If you can help other Residents with topics such as Word, Wordpad, Notepad, browsers, email, etc., please send me an email at wvcomputerclub@gmail.com. We need your help.

MAC SIG Steve Lynn, head of the Mac SIG group, is looking for suggestions as to how the Computer Club can better support Mac users. If you have ideas that can help Steve formulate a plan for supporting Mac users, please send them to him at slynn15@icloud.com. Information Central has been modified based on Steve's recommendations. In the center column of Information Central is a feature called *For MAC Users*. It contains information applicable to Apple computers. Let Steve know if you have suggestions for other beneficial information links that might be added to the area *For MAC Users*. Watch the *Weekly Insider* for meetings of the Mac SIG Group.

Recycling Ed Dahrsnin and his team are accepting working computers and components for recycling, but no CRT monitors. Let Ed know if you would like to help recycle

(Continued on page 4)

President

(Continued from page 3)

computers. Ed and his team meet on Monday afternoons at Manor North. Working in the recycling effort may also help you when you have problems. Thanks to Ed and his team, the Computer Club has given **166** computer systems to the Lampeter-Strasburg School District for families that cannot afford a computer for their students and two laptops to the Hand Middle School in Lancaster for their Science classroom.

Thank You My thanks to all of you who volunteer your time and knowledge to help other Residents. We need more volunteers! •

Sysinternal's Process Explorer by Sid Paskowitz

The following article is for the more technical members of the Computer Club and you may find it difficult. However, reading articles like this may give you understanding of something that you didn't understand before. *Editor*

Introduction The information in this document is based on my understanding of Process Explorer and my use of it. Please note the information and displays below are subject to update or change and were applicable when this document was written. All the actions and displays were created using a 64-bit Windows 10 computer. Please send comments or suggestions for improving this document to wvcomputerclub@gmail.com.

Why I Use It The following instructions describe the process for installing and running Sysinternals Process Explorer on a personal computer (PC). I have found Process Explorer to be a handy tool when, due to something I have done or when something happens unexpectedly, I suspect something unwanted is happening on my computer. When that happens, I run Process Explorer from my taskbar to determine if a virus is running on my computer.

An Overview Process Explorer is different from other anti-malware programs. Programs such as Malwarebytes and Windows Defender scan the computer's storage drive(s) to determine if malicious code is embedded on a drive. Process Explorer takes a "snapshot" of the code running on the computer and sends that "snapshot" to multiple reviewers to see if any reviewer finds any segment of the running code to be malicious or questionable. That process is quick and efficient, but it only displays a problem when malicious code is running when the "snapshot" is taken and will not show if malicious code is hiding elsewhere on the computer. When malicious code is found, Process Explorer may provide help for correcting the problem. I run Process Explorer from my taskbar because it is always accessible at the bottom of my computer screen.

(Continued on page 5)

Process Explorer

(Continued from page 4)

Installation The download site for Process Explorer is <https://technet.microsoft.com/en-us/sysinternals/processexplorer.aspx> as shown in the following display. Left-click on the download link (see arrow below) to download the program.

Process Explorer v16.2

By Mark Russinovich

Published: February 17, 2017

 [Download Process Explorer \(1.8 MB\)](#)
Rate: ☆☆☆☆☆

Share this content  

Download



[Download Process Explorer](#)
(1.8 MB)

[Run Process Explorer](#) now from Live.Sysinternals.com

Runs on:

• Client: Windows Vista and higher (Including IA64).

The downloaded file is a zipped file that can be opened (unzipped) by left-clicking (or double-left-clicking) on the file name ProcessExplorer.zip in the Download folder as shown below:

 ProcessExplorer.zip 4/23/2017 12:46 PM Compressed (zipped) Folder 1,876 KB

When I unzipped the file, it created a Process Explorer folder in my Documents folder:

 ProcessExplorer 4/23/2017 12:39 PM File folder

When I opened the Process Explorer folder I got the following display:

| Name | Type | Compressed size | Password ... | Size | Ratio | Date modified |
|---------------|-------------------------|-----------------|--------------|----------|-------|-------------------|
| Eula.txt | Text Document | 4 KB | No | 8 KB | 59% | 3/3/2016 8:44 PM |
| procexp.chm | Compiled HTML Help file | 64 KB | No | 71 KB | 11% | 2/2/2017 11:32 AM |
| procexp.exe | Application | 1,178 KB | No | 2,648 KB | 56% | 2/2/2017 11:45 AM |
| procexp64.exe | Application | 632 KB | No | 1,419 KB | 56% | 2/2/2017 11:39 AM |

(Continued on page 6)

Do This and Your SSD Will Last Much Longer by Martin Klaver

When Windows is in sleep (hibernation) mode, it may slow the performance of solid state hard drives or interfere with shared printing. Here is the fix:

Type *Windows key + X*, select Windows Powershell (Admin), and answer “yes”.

Then, type *powerconfig -h off* and press enter.

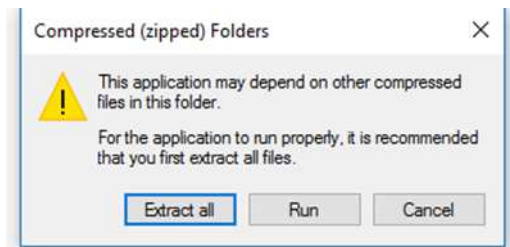
That is all there is to it. •

Process Explorer

(Continued from page 5)

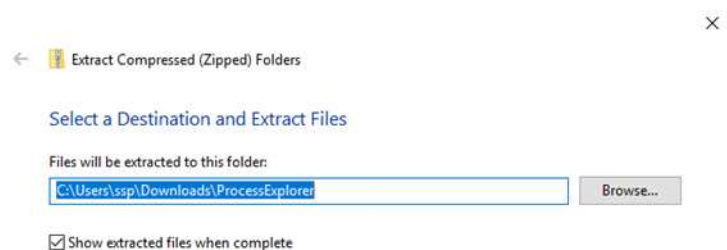
It was not clear which .exe application file I should click on, so I chose the one with the larger size in hope of it having more content and capability (see previous page). It is also possible that the file procexp64.exe is only to be used on 64-bit PCs, so to be on the safe side for all users, I chose procexp.exe as the preferred application.

When I clicked on the larger procexp.exe file name, I got the display to the right, and based on its recommendation, I clicked in the box to Extract all:



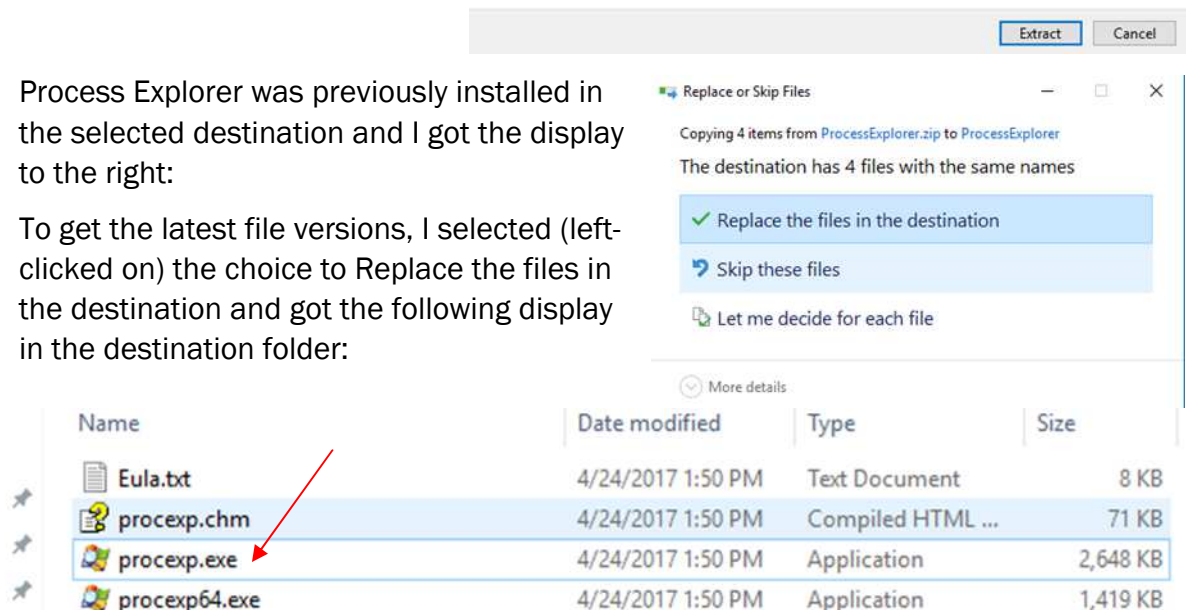
I then got the display to the right that asked where I wanted to put the extracted files.

I could have changed the destination or browsed for a different destination, but I made a note about the destination selected for use as explained below, and I clicked in the Extract box.



Process Explorer was previously installed in the selected destination and I got the display to the right:


To get the latest file versions, I selected (left-clicked on) the choice to Replace the files in the destination and got the following display in the destination folder:

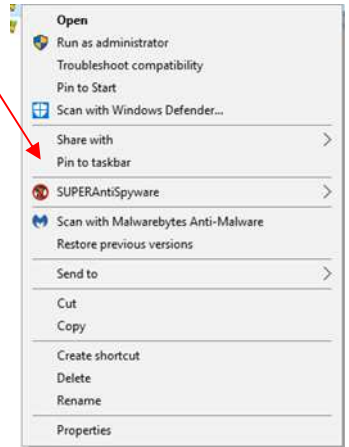


(Continued on page 7)

Process Explorer

(Continued from page 6)

I right-clicked on the icon for the larger application file and got the window to the right where I clicked on Pin to taskbar. That action put the Process Explorer icon  in the taskbar.



When To Use As mentioned earlier, whenever I suspect a problem on my computer that may be associated with malware, I left-click on the Process Explorer icon on the taskbar. (See the icon above.)

That action should result in the following partial display. (If not, see next page) The arrow points to the notation that hash code has been submitted.

| Process | CPU | Private Bytes | Working Set | PID | Description | Company Name | Virus Total |
|-------------------------|---------|---------------|-------------|------|----------------------------------|-----------------------|-------------------|
| System Idle Process | 98.35 | 0 K | 4 K | 0 | | | |
| System | | | | | | | |
| Interrupts | 0.10 | 136 K | 5,896 K | 4 | n/a Hardware Interrupts and DPCs | | |
| smss.exe | 0.19 | 0 K | 0 K | 444 | | | |
| Memory Compression | | 428 K | 1,172 K | 444 | | | |
| csrss.exe | < 0.01 | 0 K | 8 K | 2656 | | | |
| wininit.exe | | 1,720 K | 6,436 K | 596 | | | |
| services.exe | | 1,324 K | 5,376 K | 688 | | | |
| svchost.exe | | 4,976 K | 8,448 K | 828 | | | |
| WmiPrivSE.exe | | 11,844 K | 25,820 K | 932 | Host Process for Windows S... | Microsoft Corporation | Hash submitted... |
| unsecapp.exe | | 3,280 K | 10,524 K | 3124 | | | |
| RuntimeBroker.exe | < 0.01 | 1,152 K | 6,320 K | 3232 | | | |
| ShellExperienceHost... | | 19,288 K | 37,260 K | 4516 | Runtime Broker | Microsoft Corporation | Hash submitted |
| SearchUI.exe | | 31,972 K | 62,088 K | 4980 | Windows Shell Experience H... | Microsoft Corporation | Hash submitted |
| RemindersServer.exe | Susp... | 53,672 K | 98,988 K | 5156 | Search and Cortana applicati... | Microsoft Corporation | Hash submitted |
| SpeechRuntime.exe | Susp... | 11,336 K | 18,672 K | 5844 | Reminders WinRT OOP Ser... | Microsoft Corporation | Hash submitted... |
| ApplicationFrameHost... | 0.18 | 26,996 K | 20,476 K | 5852 | Speech Runtime Executable | Microsoft Corporation | Hash submitted... |
| smartscreen.exe | | 4,292 K | 18,544 K | 6000 | Application Frame Host | Microsoft Corporation | Hash submitted |
| svchost.exe | | 8,500 K | 14,844 K | 6304 | SmartScreen | Microsoft Corporation | Hash submitted... |
| svchost.exe | | 5,016 K | 10,636 K | 1008 | Host Process for Windows S... | Microsoft Corporation | Hash submitted... |

As shown by the arrow in the figure on the next page, after a short period following when the code "snapshot" is sent to a number of reviewers, those reviewers respond and their results are tabulated. When malicious code is reported, the number of reviewers reporting malicious code is shown in red. In this example, below, no malicious code was found.

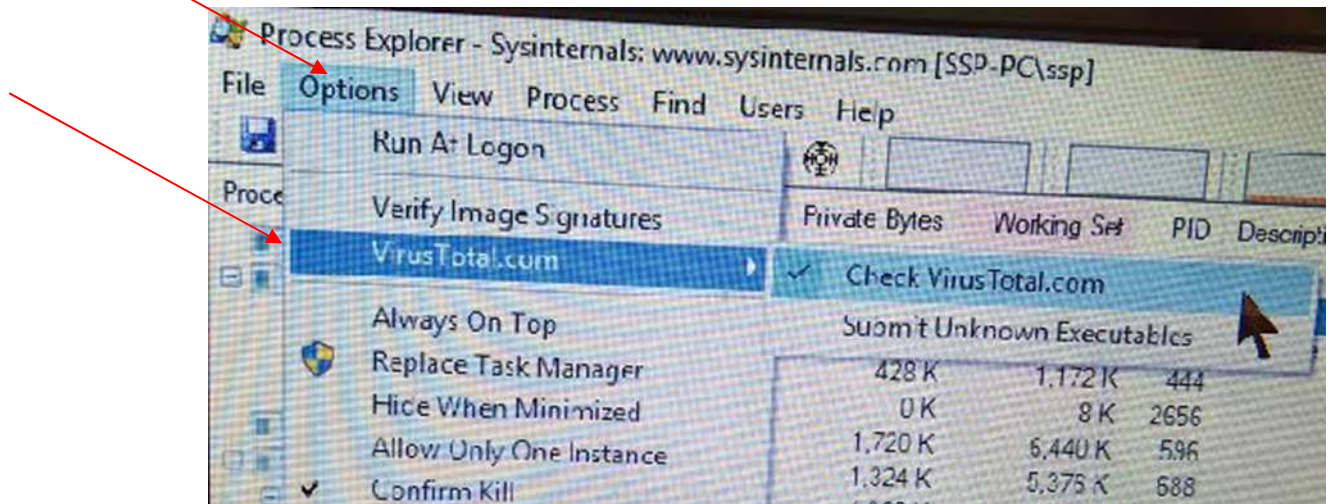
(Continued on page 8)

Process Explorer

(Continued from page 7)

| Process | CPU | Private Bytes | Working Set | PID | Description | Company Name | VirusTotal |
|-------------------------|---------|---------------|-------------|------|---------------------------------|------------------------|------------|
| System Idle Process | 96.38 | 0 K | 4 K | 0 | | | |
| System | 0.07 | 132 K | 1,084 K | 4 | | | |
| Interrupts | 0.19 | 0 K | 0 K | n/a | Hardware Interrupts and DPCs | | |
| smss.exe | | 360 K | 1,008 K | 440 | | | |
| Memory Compression | | 0 K | 8 K | 2772 | | | |
| csrss.exe | | 1,800 K | 6,376 K | 588 | | | |
| wininit.exe | | 1,040 K | 5,264 K | 680 | | | |
| services.exe | | 3,568 K | 7,892 K | 812 | | | |
| svchost.exe | | 10,048 K | 24,752 K | 924 | Host Process for Windows S... | Microsoft Corporation | 0/60 |
| WmiPrvSE.exe | | 2,888 K | 10,236 K | 3176 | | | |
| unsecapp.exe | | 1,220 K | 6,392 K | 3356 | | | |
| RuntimeBroker.exe | | 12,044 K | 34,532 K | 4424 | Runtime Broker | Microsoft Corporation | 0/61 |
| ShellExperienceHost... | Susp... | 33,300 K | 73,196 K | 4500 | Windows Shell Experience H... | Microsoft Corporation | 0/60 |
| SearchUI.exe | Susp... | 47,648 K | 92,552 K | 5156 | Search and Cortana applicati... | Microsoft Corporation | 0/61 |
| SpeechRuntime.exe | 0.17 | 27,480 K | 23,228 K | 5900 | Speech Runtime Executable | Microsoft Corporation | 0/62 |
| RemindersServer.exe | Susp... | 11,408 K | 18,692 K | 5964 | Reminders WinRT OOP Ser... | Microsoft Corporation | 0/62 |
| smartscreen.exe | | 8,568 K | 14,892 K | 932 | SmartScreen | Microsoft Corporation | 0/61 |
| svchost.exe | < 0.01 | 5,836 K | 13,468 K | 1000 | Host Process for Windows S... | Microsoft Corporation | 0/60 |
| svchost.exe | | 21,588 K | 53,024 K | 528 | Host Process for Windows S... | Microsoft Corporation | 0/60 |
| sihost.exe | | 5,864 K | 20,972 K | 4136 | Shell Infrastructure Host | Microsoft Corporation | 0/60 |
| SynTPEnh.exe | < 0.01 | 5,588 K | 1,008 K | 4208 | Synaptics TouchPad 64-bit ... | Synaptics Incorporated | 0/58 |
| taskhostw.exe | < 0.01 | 13,424 K | 26,576 K | 4232 | Host Process for Windows T... | Microsoft Corporation | 0/61 |
| ToshibaServiceStatio... | | 60,756 K | 3,384 K | 7956 | TOSHIBA Service Station | TOSHIBA Corporation | 0/56 |

If after left-clicking on the Process Explorer icon on the taskbar as described earlier, the display does not show that hash code has been submitted, left-click on the Options link as shown by the arrow in the figure below, then left-click on VirusTotal.com and Check VirusTotal.com in the box as shown by the red outline. That should produce the screens shown earlier.



How To Use If a significant number of reviewers report malicious code, click on the red link(s) and follow any instructions provided by the program. Other security programs such as Malwarebytes and Windows Defender or Security Essentials should also be run. If no malicious code is reported, close Process Explorer and continue what you were doing. •

The Equipment Corner by Ed Dahrsnin

Refurbished Systems

The following systems are available for club members:

519 HP Pavilion AV976VA, Windows 8.1 (x64), Tower

520 Dell Inspiron 530s-21QTZD1, Windows 7 Pro, Tower

522 C2I MS-7210, Windows 10 Pro (x64), Tower

523 HP nx9420, Windows 7 Home (x64), Laptop

524 Dell Inspiron 530s, Windows 10 Pro, Tower

Miscellaneous We have 3 volt CR2023 batteries (suitable for motherboards to keep the system clock running) and a variety of CD-ROM's, floppy disk drives, keyboards, 2-button mice, various power supplies, and assorted cables. Please contact Ed Dahrsnin at 464-6591.

Donations We continue to accept printer cartridges and laptop computers with power adapters. We accept only working printers with drivers and documentation. Also, we accept only working monitors. Cathode Ray Tube monitors are not acceptable. Stand-alone scanners are not acceptable. Bring the items to Manor North's recycle closet on the fifth floor of 'J' building on Monday only, from 1pm to 1:30pm. •

The Mission

The Mission of the Willow Valley Computer Club is to:

- Provide the means to educate beginners or interested non-users on how to use a computer.
- Arrange for speakers to talk to the Club about subjects that would be of interest to those with some background and experience in computer use.
- Provide a forum for interchange of computer information among members.

For more information about the Club, contact Sid Paskowitz at 464-2127 or wvcomputerclub@gmail.com •

The Leadership

Officers

President: Sid Paskowitz

Vice President: Peter Scott

Secretary: Marge Schmieder

Treasurer: Charlie Trumbo

Community Representatives

Manor: Larry Gallagher

Manor North: Lee Yermuth

Lakes: Gene Simasek

Providence Park: Peter Scott

Willow Gables: Cathy Thorn

Committee Chairpersons

Program: Peter Scott

Training: Ralph Beedle

Equipment: Ed Dahrsnin

Technical Support: Tony Poulos

Website: Sid Paskowitz

Publicity: Wally Gordon

Newsletter: Al Williams

Mac Interest Group: Steve Lynn

Computer Room Coordinators:

Gene Simasek Lee Wermuth

Microsoft Liaison: Ed Dahrsnin

Past Presidents

Larry Gallagher

Reviewer Acknowledgment

The following individual kindly reviewed this issue:

Sid Paskowitz

Thank you,

Al Williams

Interested in reviewing the Computer Club newsletter before it goes to press, providing advice about the content, or writing an article? Please contact:

Al Williams at atwilliams136@gmail.com