



INNOVEST SME

Accelerating Small Business

Safe Digital Technology Engagement

Rick Chisholm and Tala Chisholm

COPYRIGHT NOTICE

Copyright © 2018 by Innovest SME

All rights reserved. No part of this publication may be reproduced, distributed, or transmitted in any form or by any means, including photocopying, recording, or other electronic or mechanical methods, without the prior written permission of the publisher, except in the case of brief quotations embodied in critical reviews and certain other non-commercial uses permitted by copyright law. Permission requests should be submitted to the publisher in writing at one of the addresses below:

30/192A Kingsgrove Rd
Kingsgrove, NSW 2208
Australia

Phone: +61 2 8007 2907

E-mail: admin@innovestsme.com.au

Website: www.innovestsme.com.au

CONTENTS

	Preface	4
1	What Is Digital Citizenship?	7
2	Being a Good Citizen	13
3	Best Practices for Sharing	18
4	Networking and Personal Branding (I)	24
5	Networking and Personal Branding (II)	29
6	Digital Security and Safety (I)	35
7	Digital Security and Safety (II)	41
8	Dealing with the Dark side	47
9	Digital Etiquette (I)	53
10	Digital Etiquette (II)	59

PREFACE

The Internet has changed the way that people connect, communicate, and conduct business. The digital age has provided many benefits, but it does have a downside. Given the sheer volume of digital information that we send and receive each day, it is important to learn basic citizenship skills. These skills will help prevent missteps and keep your digital relationships running smoothly.

*If you don't understand
digital communication
you're at a disadvantage.*

BOB PARSONS



WHAT IS DIGITAL CITIZENSHIP?

Mike Ribble defines digital citizenship as using technology responsibly and appropriately. Anyone who interacts regularly online automatically becomes a digital citizen. Like any other community, digital citizenship requires members to behave in a mature and civil manner. Good citizens ensure that digital users have safe and pleasurable experiences.

WHAT IS DIGITAL CITIZENSHIP?

Digital citizens all belong to the digital society, and they need to adhere to the norms and rules that have been established. There are nine elements that people experience when they interact online. These interactions define what occurs in digital citizenship.

Nine Normal Elements:

- **Access** – Citizens have different levels of access. Full access should be a goal of citizenship.
- **Commerce** – Buying and selling online is increasing, and consumers need to be aware of what they purchase and the legality of their purchases.

- **Communication** – There are numerous ways to communicate online, and citizens need to make wise decisions in what and how they communicate.
- **Literacy** – Technological literacy requires people to keep up with digital changes.
- **Etiquette** – Citizenship comes with a responsibility to follow etiquette when communicating with others.
- **Law** – Citizens have a responsibility to behave ethically and be aware of laws governing them.
- **Rights and Responsibilities** – The rights of users are shared equally. These rights come with responsibilities.
- **Health and wellness** – Physical and psychological issues can occur when ergonomics and other problems are not addressed.
- **Security** – Citizens must take action to protect their information online

ENGAGING WITH OTHERS

Digital media allows us to communicate, collaborate, learn, and share online. When engaging with others online, it is important to behave as though they are in the room with you.

Tips to Engage:

- **Be patient** – Build relationships slowly. Aggressive attempts at communication can make people uncomfortable.

- **Dialogue** – Ask and answer questions to begin discussions.
- **Share sparingly** – It is important to share information, but be careful not to spam people.
- **Maintain relationships** – Build new friendships, but be sure to pay attention to existing relationships.
- **Be respectful** – Unless you are video chatting, it is difficult to convey tone. If you are not sure if something is respectful, do not type or say it.

IT'S A MOVING TARGET

Our digital lives are constantly evolving. The changes in technology are rapidly occurring, and our lives are shifting at a great pace. Over the past few decades, technology has changed the way we work, shop, and communicate. Social media is relatively new, but it is an integral part of society. As technology changes, the way we interact changes along with it. It is imperative that we pay attention as our tools change in order to remain relevant in our work and social lives. The target of technology is constantly changing, and we need to change with it.

BELONGING TO A COMMUNITY

The ability to communicate is easy, inexpensive, and instantaneous in a digital world. Distance no longer limits our communication.

Methods of communication:

- Text
- FaceTime
- Email
- Social media
- Instant messaging

Because communication is essential to any community, the digital world can help improve communities. Digital citizens are citizens of the Internet, and they are citizens of their personal and professional communities. When you are part of any community, you have a responsibility to communicate respectfully and expand relationships. Invest in your digital relationships with your time and interest. Remember that it takes time for a strong community to develop.

PRACTICAL ILLUSTRATION

Delia was determined to improve her online presence and improve her networking skills. She decided to send updates about her company twice a day. After a week, she noticed a decline in comments and responses. After speaking with a friend, Delia learned that she shared so much information that people began to ignore her posts.

*If a man be gracious and
courteous to strangers,
it shows he is a
citizen of the world.*

FRANCIS BACON



BEING A GOOD CITIZEN

Being a good citizen is important both online and off. The rules of citizenship for each are similar. When using digital technology, remember to be positive and helpful, and apply what works in real life in the digital realm. If you try to be a good person, your path to becoming a good digital citizen will be much easier.

BUILD IT UP

Your tone will define your digital presence. No matter the content that you produce or communication you make, it is essential that you attempt to remain positive. Build up your community, and avoid negativity. Positive content generates more traffic than negative content. This is because people will share positive content with their friends and family, which grows your community.

You will draw people to you if they feel that you are able to help them. Provide useful information and tips. Invite people to ask questions, and develop a respectful dialogue. This cements relationships and leads to repeat viewings and communication. When are a good digital citizen, you encourage good citizenship in others.

REAL WORLD INFLUENCES

Real world influences are useful when examining your digital citizenship. If you are a good citizen in real life, you will be a good digital citizen. Consider what makes a good public citizen. Examples include participation, civility, meeting responsibilities, and obeying laws. Translate your real world ideas into your conduct online. This will guide you and prevent you from making unnecessary mistakes in your online conduct.

USE TECHNOLOGY APPROPRIATELY

Technology needs to be used responsibly. All activity needs to be both legal and ethical. How you use technology will depend on where you are and what you are doing. For example, it is unethical to download and play games on your computer at work, but it is perfectly acceptable to do so at home. You should also be careful with any technology that you borrow from your friends. If you use something that does not belong to you, avoid unapproved downloads, rude communication, and any questionable activity.

There are basic rules and laws that govern digital citizenship. For example, the Internet is not free. Using a neighbor's connection is not only illegal; it is inconsiderate because it slows the Internet speed for paying customers. Additionally, you should avoid pirated software, music, movies, etc. These downloads are illegal, and some questionable websites increase your chance of contracting a computer virus. If you are in question whether an action is ethical or legal, play it safe and don't do it.

THE GOLDEN RULE

Treating others the way that you would like to be treated is the golden rule. This should be applied in all areas of life, including your digital life. You need to treat yourself and others with respect. This does not mean that you are dishonest or weak. It simply means that you remain civil in your interactions with other people. Do not communicate in a way that you would consider rude or disrespectful as the receiver. Obeying the golden rule sounds easy, but many problems occur because this rule is ignored. Think before you communicate; do not act out of emotion.

PRACTICAL ILLUSTRATION

Thomas decided to increase his productivity. He read an article that said short, frequent breaks were good for focus and productivity. He set an alarm so that he would remember to take a break every hour so he could take a break with an online computer game. By the end of the week, he realized that he was less productive than before. When he looked back at the time he spent working, Thomas realized that his breaks were lasting 20 minutes to an hour.

*The internet is becoming
the town square for the
global village of tomorrow.*

BILL GATES



BEST PRACTICES FOR SHARING

It is easy to share information online and that many people do it without considering the consequences. It is possible, however, to share too much. What we put online in unguarded moments can haunt us for the rest of our lives. This is why digital citizens need to be mindful of what they share, who they share it with, and how they share it.

DIGITAL FOOTPRINTS

Every time you access the Internet you leave a digital footprint. Digital footprints are a history of everything you do online. They come from what you share and data collected on your sites visited, and they do not go away. Retailers use your digital footprint to target coupons and special offers to the right customers based on what they look up and what they purchase. Companies look at digital footprints of current and potential employees. This is why you must be mindful about what you share. Remember that a digital footprint can last forever. Something you thought you removed could cause problems for you later.

PERSONAL AND WORK LIVES

The digital world has blurred the line between our personal and professional lives; they are much thinner and easier to cross. Social networks, specifically, allow us to include colleagues and coworkers in our personal lives. While networks can help develop deeper relationships with coworkers and give them a glimpse of your life outside of work, it can also cause problems.

You never know what information that you share with your friends or coworkers will be seen by your supervisors. Companies use social media as a tool to monitor employees. Complaining about work and venting online can risk your career. Although some people find it restrictive, it is important not to share information that could be offensive.

STOP AND THINK BEFORE YOU POST

In a digital world, it is easy to accidentally share something that could easily be misinterpreted. Sharing videos, pictures, and thoughts is so simple that many people do not think about what they are doing. Careers and relationships could be preserved if people would simply stop and think before they post. There is no reason to post everything that you do.

Before you post anything, ask yourself if you want your family and ALL of your friends to see it. If the answer is no, DO NOT POST IT. Too often, people have what should be private conversations in the public comment section of social media. If you want to address an individual, use a private message. Additionally, it is a good idea not to share anything with people

you do not know and trust. There is nothing to prevent people you share things with from sharing them with others.

DO NOT OVERSHARE

One of the main problems in the digital realm is oversharing. First, not everything is meant to be shared. You are better off keeping personal information private. It is unattractive when people share every thought or experience that they have on social media for all to see. This action appears self-indulgent and immature, and it is difficult to trust someone who does not have a filter.

Choose what you share wisely. Remember that you are on a public forum, and your personal life does not need to be there. Additionally, you need to avoid statements that could be controversial or offensive. For example, you should think carefully before making any comment about political parties, religions, or people groups. The Internet is a diverse place, and it is easy to make comments that could be misunderstood. This is why so many celebrities have to publically apologize because of their tweets.

Finally, no one cares about every day, mundane activity. Sharing too much boring information will clutter the notifications of your friends and followers. This can lead to people severing digital ties or ignoring everything that you share online. Either way, sharing too much can become the equivalent of not sharing anything at all.

PRACTICAL ILLUSTRATION

Jerry was active on social media. He constantly posted pictures and added new friends and followers. He won tickets to a concert, but he needed to leave work early to make it in time. Jerry lied and told his boss that he had food poisoning. The next day, Jerry's boss called him into the office and fired him. One of Jerry's coworkers, who was friends with Jerry's boss, made a comment on a photo from the concert. The comment allowed Jerry's boss to see the picture and discover the truth. Along with firing him, Jerry's boss also informed him that he would have let Jerry leave early if he had asked.

*Your name and face
carry your brand both in
reality and virtual reality,
such that wherever they
are cited, your personal
brand is at stake.*

DAN SCHAWBEL



NETWORKING AND PERSONAL BRANDING (I)

Digital citizenship is a large part of networking and personal branding. This requires you to monitor your online presence and be careful in the way that you present yourself. If you are proactive in your sharing, persona, and social networking, you will be able present an effective online image that helps you create social connections.

PERSONAL BRANDING

The first step in personal branding is defining your brand. These questions will define your brand and help you market yourself. When you create your personal brand, it is essential that you remain consistent with your shares and posts. This is why you need to be mindful in what you post and think about what you are communicating. Do not shift your message or tone. This will cause people to question your sincerity.

Ask yourself:

- What are my skills?
- What is my message?
- Who is my audience?

BE YOURSELF

Whether you are online or offline, it is important that you be yourself. People are attracted to sincerity; so only communicate something if you genuinely believe it. People who come across as insincere or fake are not easily trusted. It is important that you communicate honestly in person and in your online persona. When you are yourself, you know that people in your network are drawn to you and your message, not a fictional character.

Remember, there is such a thing as oversharing, so it is important that you establish professional boundaries when you are being yourself.

SOCIAL NETWORKING

Social networking is essential to your branding. When done correctly, social networks are useful tools that expand your community. When not used correctly, social networking can have lasting, damaging effects.

- **Choose the right networks** – Choose networks that your customers use. You cannot effectively use them all.
- **Post regularly** – Post at regular intervals to keep the attention of your audience.
- **Monitor it** – Monitor your social networks and respond to comments and questions.

IF YOU SHARE IT, EXPECT EVERYONE TO SEE IT

When you share something online, expect everyone to see it. You must come to the realization that there is no such thing as privacy online. Do not be fooled by the ever-changing privacy settings that social networks have. What you share online can and will be shared by other people. It only takes seconds for a post to be shared or a screenshot to be taken. Even if you remove a post, the damage may already be done. This is why thinking before posting cannot be emphasized enough.

PRACTICAL ILLUSTRATION

Michelle was having difficulty building her network online. She joined every social media platform she heard about, and she began a blog. She made sure to check on them each week. Unfortunately, hardly anyone responded to her posts. In an effort to improve traffic, she tried changing her tone, persona, and the topics she addressed. Over time, however, traffic seemed to drop even more. She wasn't sure what else she should try.

*Networking is marketing.
Marketing yourself,
marketing your
uniqueness, marketing
what you stand for.*

CHRISTINE COMAFORD-LYNCH



NETWORKING AND PERSONAL BRANDING (II)

Networking and branding requires more than engaging in social media. It requires the relationship building. Digital media makes it easier to introduce people to each other, volunteer, communicate, and monitor your reputation. All of these activities are essential to your personal brand. When done correctly, you will find networking to be much easier.

INTRODUCE COLLEAGUES

Networking requires give and take. While you network to meet new people, you also need to facilitate meetings between colleagues as well. If you know two people who would benefit from meeting each other, introduce them. Consider hosting mixers or other parties to help people meet each other in person and put faces to names.

It is also possible to introduce people via email. It is a good idea to discuss the idea with your friends before sending the email so that you are going to introduce them so that the email does not come as a surprise. Introducing people online can make it easier for them to meet in person.

Email Example:

Subject: Sam meet James; James meet Sam

Sam, I would like to introduce to James. He has been a graphic designer in our department for three years, and I believe that you could benefit from his expertise in layout and design.

James, Sam is a senior editor with the eBook division. I know that you spent a great deal of time assisting his artists with the new software.

Sam, I know that your department is having difficulty with the change in software, and James could help with the transition.

Good luck,

Sharon

VOLUNTEER TO HELP OTHERS

Helping others and volunteering is good for people in your network and for you. Helping others does not have to be complicated or time consuming. Simply find out who needs a favor and volunteer your services. It is a good idea to share on social media when you volunteer your time and services. This encourages other people to volunteer with you, and it shows your network that you are willing to help the people who are in your network.

You should also consider volunteering in your community. This helps you meet new people with similar interests. It also provides you with the

opportunity to learn new, marketable skills. Many companies prefer to hire and advance people who actively volunteer.

BLOG

“Start a blog” is advice commonly given to professionals who want to expand their networks. Blogs are only effective when they are done correctly. It is better not to start a blog than to begin one that you have no interest in maintaining.

How to Blog:

- **Make a point** – Only blog if you have something to share.
- **Be thorough** – Proofread your posts for accuracy and grammar.
- **Be consistent** – Update your blog on a regular basis.

Blogs require commitment. If you take the time to post regularly, it can benefit your personal brand.

GUARD YOUR REPUTATION

Reputations are made or destroyed online. You need to guard your reputation carefully because it is valuable. There are steps you can take to guard and defend your reputation:

- **Monitor your online activity** – Make sure that your accounts are not hacked.

- **Keep information private** – Do not share any personal information.
- **Be careful lending technology** – People can pose as you when using your technology.

If your reputation becomes damaged for any reason, you need to defend it. Address any misinterpretations other people make, and issue apologies if necessary.

Finally, you need to promote your reputation. Do this by sharing your successes and posting testimonials and recommendations from others.

PRACTICAL ILLUSTRATION

The food bank was low on volunteers and asked several businesses to lend a hand. Glen decided to volunteer at the local food bank with his colleague. At first, he was not sure about work, but he enjoyed himself and he made contacts while he was there. Glen posted pictures online and found himself invited to other volunteer functions. He and his coworker developed a volunteer program at work. After a few months, Glenn saw his responsibilities increase.

*If you reveal your secrets
to the wind, you should
not blame the wind for
revealing them to the trees.*

KAHLIL GIBRAND



DIGITAL SECURITY AND SAFETY (I)

Being a good digital citizen requires you to be responsible for your own security and safety. Cybercrimes happen every day. When you are online, you need to practice the same level of vigilance that you do when you are interacting in the real world. Be slow to trust new people, and implement security software and other precautions to protect your information.

DON'T TRUST ANYONE YOU DON'T KNOW

The Internet is just like any other place. It is possible to meet wonderful people and develop useful contacts online. There are, however, many malicious people who are looking for opportunities to steal and exploit personal information. When you are online, do not put your trust in anyone you do not know. Internet scammers are professionals, and are very good at manipulating people, so be aware.

Signs of a scammer:

- You are asked to download something.
- You are given a link to something.
- An offer seems too good to be true.

- You are asked for money.
- You are asked for personal information.
- You are promised money.

ENABLE 2-STEP VERIFICATION PROCESSES

Password accounts are commonly hacked, and you do not have to be a computer genius to hack emails. In fact, there are numerous online tutorials on how to hack an email account.

There are precautions that you can take to limit your risk online. Many email accounts and other sites offer a 2-step verification process. If you have access to this service, use it. The process is simple, and it helps prevent the theft of your passwords. After signing up, you will enter your password, and a verification code will be sent to your phone. You will only be able to access your account after entering the code. It is possible to establish your home computer and request that the code not be needed to log in on it. The code would still be required from other locations, making it difficult for someone else to hack your account.

PUBLIC WI-FI

Public Wi-Fi is great for the person on the go. You must, however, take extra precautions when using public Wi-Fi. This type of connection does not have the same security that your personal Internet account does because there are numerous users. When you use public Wi-Fi, avoid accessing sensitive information, like your bank account.

Public Wi-Fi Security:

- **Turn off sharing:** For a MAC, this is under system preferences. For a PC, this is under HomeGroup of the Network and Internet settings in the control panel.
- **Firewall:** Make sure that your firewall is turned on.
- **Confirm the network:** Hackers set up fake networks. Make sure that you connect to the correct Internet account.
- **Use sites with SSL:** SSL or secure sockets layer requires a certificate and keeps private information secure.
- **Use VPN:** VPNs make sure to route through secure sites.

PUBLIC COMPUTERS

With the popularity of laptops and smartphones, it is often possible to avoid using public computers. There may be times, however, when you find yourself using public computers. There are a few tips to help keep your information secure:

- **Do not save login information:** Always choose the option not to save your login name or password, and make sure that you log out when done
- **Erase your history:** Disable settings that save passwords and delete your Internet history when done.
- **Be aware of your surroundings:** Do not leave the computer unattended, and keep an eye out for people watching your screen.

- **Mind what you do:** Never enter personal or sensitive information, like credit card info, on a public computer.

PRACTICAL ILLUSTRATION

Sally traveled for work, which required her to use public Wi-Fi quite frequently. She had virus software on her computer and never questioned her security. One day she logged onto “free airport Wi-Fi” while waiting for a plane. It was her nephew’s birthday, so she decided to order his present with her spare time. The next day, her credit card company called to ask her about some suspicious account activity. Someone had used her credit card account to make thousands of dollars in purchases.

*In God we trust.
All others, we virus scan.*

ROBBIE SINCLAIR



DIGITAL SECURITY AND SAFETY (II)

Digital security and safety requires users to monitor email attachments, use strong passwords, back up files, and update software. Taking these steps will make you proactive in your digital citizenship and protect your personal information online.

EMAIL AND ATTACHMENTS

We use email for work and personal reasons every day. Emails and their attachments, however, are regularly used to hack computers. Just because you receive an email from someone you know, does not mean that the email is safe. Once an account is hacked, it is used to send messages to the contact list. If you receive an email that seems odd, contact the sender before clicking on any links or opening any attachments.

Once you download an attachment, the damage is done. Before downloading or clicking on anything, hover over the link and check to see that the link you see and the link you are being directed to match. Never click a link or download an attachment unless you are sure that they are safe. If you accidentally click something, run a virus scan, preferably in Safe Mode.

PASSWORD RULES

Hacking often occurs because people choose the wrong passwords. Using the same password for everything, using easy passwords, and keeping the same passwords for years will put your account at risk. There are a few key points to choosing strong passwords. Typically an eight character password minimum with ten characters a normal recommendation. They must include:

- Uppercase letters
- Lowercase letters
- Numbers
- Symbols/characters

BACK UP YOUR FILES

It is essential to back up your files regularly. You never know when a computer will crash, or if your computer will be stolen. Backing up files protects your information. How often you back up your files will depend on how regularly you use your computer. Files should be backed up daily, weekly, or monthly. There are different backups.

- **Full back up** – This type of backup takes the most time and storage space. It is the fastest to restore.
- **Incremental backup** – These backups changes made after the latest backup. It is faster to backup, but it takes longer to restore.

- **Differential backup** – The backup occurs after the latest full backup. It does not take long to backup, and it restores slower than full and incremental backup.
- **Mirror** – Files deleted in the computer are also deleted on the backup.
- **Local** – Backups in the same building such as external hard drives, etc.
- **Online** – It is possible to backup files online. It is safe in the case of natural disasters but it is slow to restore.

UPDATE YOUR SOFTWARE

It is important to update your software regularly. Software companies frequently update their programs to fix bugs and address security threats. If you do not update your software regularly, you risk your programs running slower than normal and contracting malware and viruses. You should check for updates regularly. A good rule of thumb is to check for updates every time that you turn on your computer for the day. This way, you have any updates completed before you begin your work. Make sure that you update virus software, OS, firewall, iTunes, Microsoft Office, etc.

PRACTICAL ILLUSTRATION

Stan was working on a major project. He spent weeks staying up late trying to make the deadline. He was careful to back up the hard drive every day. A week before the project was due, Stan's computer crashed

because of a virus. He was able to recover some of the lost work, but he still lost half of his project. For the next week, he worked day and night attempting to complete the project on time. By the day of the presentation, he was exhausted. The presentation was a blur, and Stan's boss did not seem impressed.

*Cyber bullies can
hide a mask of anonymity
online, and do not need
direct physical access
to their victims to do
unimaginable harm.*

ANNA MARIA CHAVEZ



DEALING WITH THE DARK SIDE

Even though the Internet is a useful tool, it does have a dark side. Because interactions are not face-to-face, many people ignore basic civility. Harassment, trolling, and threats occur far too often online. Additionally, we all make mistakes when we address other people online. When you encounter the dark side of the digital world, you need to know how to handle the situation.

SEE IT, REPORT IT

Part of being a good citizen is addressing problems when you see them. If you see behavior that violates any user agreement or is illegal, you have a duty to report it. There are different channels for reporting violations. If you are on a social media sites, there are ways to contact administrators and supervisors. If you can't find a link to report problems, send an email to the appropriate person directly. It is important that you exercise good judgment when reporting posts. Report genuine problems, not opinions you do not like.

What to Report:

- Scams
- Bullying
- Offensive posts (lewd or foul language)
- Violent/threatening posts

BULLYING AND HARASSMENT

Bullying and harassment is a growing problem online. Unfortunately, it can escalate to violence offline. Hopefully, you never experience this problem. If you or someone you know becomes the victim of bullying or harassment, however, you need to know how to handle the situation.

- **Block and report:** Report the activity to the appropriate channels, and block the individual. This may be enough to fix the problem. Do not confront the person because this can escalate the situation.
- **Keep a record:** Keep a record of every instance of bullying and harassment. Take screenshots, save messages, and keep texts. Keep electronic and print records, and document the date and time of each occurrence.
- **Report it:** Contact the police with your evidence. Do not ignore threats. It is better to be safe than sorry.

TROLLING

Internet trolls are the bane of most digital citizens. Troll is a slang term for someone who makes comments solely to cause problems. They are not people who simply disagree or share complaints. They do not comment to engage in dialogue; they comment to get emotional responses. They delight in seeing people upset, angry, or hurt. Trolls make getting rises out of people into a game, so you need to end the game before it starts.

- **Identify trolls:** Trolls can be identified quickly. Anyone who makes rude comments, off topic comments, personal attacks, and does not listen to reason is a troll. This can typically be seen by the second or third comment.
- **Do not engage:** The saying “Do Not Feed the Troll” is common online. If you engage with trolls, you play their game. It is best to ignore them so they get bored and leave.
- **Don't take it personally:** If you do have to address a troll, do it without anger. Remember, they feed on emotion.

SHARED SOMETHING YOU SHOULDN'T HAVE?

Even careful people will occasionally post things that they regret. The first thing you must do is remove the post immediately. The faster you remove the post, the less likely it is to spread online. If a friend shared your post, ask your friend to remove it. This is why you should not be friends with complete strangers. Finally, you may contact moderators and administrators, particularly if the share violates any rules.

If you are not able to remove the post in time and it spreads, you will have to do damage control. The mature response is to take responsibility and apologize for any indiscretion. Lying and avoiding the issue will only draw out the problem.

PRACTICAL ILLUSTRATION

Diana's candle business was going well, but one commenter constantly caused her problems. The anonymous commenter was always maligning her product, calling it cheap and overpriced. Diana tried to appease the commenter, but her responses were met with insults and jokes. The commenter had no interest in being appeased. One day, Diana grew so frustrated with the commenter that she attacked her online. This only seemed to give the commenter another reason to insult her and her business on a public forum.

*Etiquette means behaving
yourself a little better than
absolutely essential.*

WILLIAM CUPPY



DIGITAL ETIQUETTE (I)

Like any other community, etiquette needs to be observed in the digital realm. It is easy to forget that actual human beings write the words we read on the computer screen. When we interact with others online, we should treat them like we would if they were standing in front of us. Keeping the topic and tone respectful will help the community run smoothly.

RESPECT AND TONE

It is important to try to be respectful when communicating. This concept is addressed in elementary school, but many adults need reminders. Remember that you are talking to a person, not the embodiment of an idea. You may disagree with someone, but rudeness and personal attacks cross the line of respectful dialogue. It may be easier to read the words aloud before drafting a response to someone. This will help you understand the writer's tone.

It is important to note that tone does not easily translate in written text. You cannot hear tone when you cannot hear the speaker. Many digital misunderstandings occur because a joke was taken seriously. It is possible for you to misinterpret the tone of a text, and it is possible for someone else to misinterpret the tone of something that you write. Reread everything that you write before posting. It is also a good idea to

have someone else look over your correspondence to identify potential misunderstandings before they occur.

SPEAK UP, NOT OUT

You are entitled to speak up when the occasion arises; this is much more effective than speaking out. Speaking up is done when there is an issue or problem, and it requires a level head. It is tempting to speak out rather than speak up. Speaking out is the act of a troll. When speaking out, logic and clarity go out the window. This occurs when we trash people anonymously. This type of communication is ineffective and only succeeds in escalating the argument.

How to Speak Up:

- Be honest
- Be calm
- Be direct

TOPICS TO AVOID

Always consider the topics that you discuss online very carefully. If you want to create controversy, bring up the topics: politics, religion, and sex. These topics are all guaranteed to polarize your audience and bring on a tidal wave of biased comments. It is best to avoid these topics in the workplace and on your professional networks.

Remember that digital media should be used to build your brand. Focus on personal and professional growth in your posts. Share ideas and discuss changes in the marketplace. Ask for feedback on new products and strategies. When you choose helpful topics, you invite dialogue that is not distracted by hot button topics.

KEEP PRIVATE MESSAGES PRIVATE

Sometimes private messages make their way into very public settings. It is easy to have complete conversations in the comments of a post. Accidentally hitting reply all when addressing a single person is a mistake that many people have made. Public forums, however, are not places to rant or publicize personal issues.

What to avoid in public forums:

- Negativity
- Personal problems
- Drama
- Conversations

If you would not discuss something with strangers, you should never put it on a social media network. Remember, there is no such thing as privacy when you are online. Keep rants and personal conversations in the ears of your friends.

PRACTICAL ILLUSTRATION

Betty was known for her wit and her sense of humor, which came out in her blog and on Twitter. Unfortunately, some people assumed that she was being serious in her posts. One day, she made a joke about a local politician's unpopular policy and caused a firestorm. People took sides on the issue, and the arguing lasted for days. She tried to remove the post, but the effects remained. Even though it was her private account, Betty found herself addressing the issue at work. Her boss was not pleased about the controversy that she created.

*Politeness and
consideration for others is
like investing pennies and
getting dollars.*

THOMAS SOWELL



DIGITAL ETIQUETTE (II)

There is more to etiquette than being polite in conversation. It requires continuing education and the ability to evaluate what is posted online. It is equally important to understand why people behave the way that they do and that everything posted online does not automatically become public domain. Finalizing your education in etiquette will give you the tools to be an effective digital citizen.

EDUCATE YOURSELF

Technology is ever changing and evolving. You are likely to see something new every day that you will not recognize. There is no reason to be embarrassed by your lack of knowledge. Simply ask about new technology or look it up online. There are numerous ways to look up technology. You can read technology journals, go to company websites, read books, and look at product reviews online. This type of education needs to occur on a regular basis. In order to be part of the digital community, you must be familiar with the tools necessary to access it.

INFORMATION PROCESSING

It is necessary to exercise critical thinking when you go online. You will read false, misleading, or partially true information. In fact, a large percentage

of information is not true. Unfortunately, people are quick to believe what they read online. Even journalists and news broadcasters have shared false information because they did not think critically and question what they saw. The key to information processing is to consider the source.

Ask the following questions to determine if the source is reliable:

- Is the information biased?
- Can you verify the information?
- Is the source reputable? (For example, the Mayo clinic)
- Is there a copyright?
- What is the purpose of the information?

Even if you use reliable sources, they are only effective if you read the complete posts. Many people only read the title before they comment. This is obvious in the comments, and it highlights the fact that they are not willing to read a few hundred words to be informed before making judgment calls.

INTERNET BOLDNESS

The Internet makes people bold because it offers some anonymity. It is possible to interact with strangers and they would not recognize us if we met in the real world. Many experts believe that this type of anonymity is what empowers Internet trolls. People often behave differently online than they do in person. They say things that they normally would not say and become bolder than normal. This boldness can cause problems when it

remains unchecked. For some people, however, Internet boldness can be helpful. For example, shy people can often communicate better online than in person. Digital citizens need to keep a close watch over their boldness. There is a line between confidence and behaving like a troll.

PERMISSION TO SHARE

Many people are under the impression that you can use anything on the Internet for any purpose. The truth is that much of the information and media online is copyrighted, which means that you need permission to share. Even if you do not see a copyright, asking someone permission to share pictures, videos, and information is digital etiquette. It is better to be told “no” upfront than to be faced with a cease and desist letter later. Always ask before you post, even if you are posting pictures of friends and family. Remember that some people are more comfortable with their pictures and information being shared than others.

PRACTICAL ILLUSTRATION

Will found a fascinating medical article and shared the information on his blog. He was thrilled when his comments tripled their usual number. Many people thanked him for the information. A doctor, however, pointed out that the study was biased and medical professionals did not perform it. Will looked up the study online and discovered that most members of the medical community dismissed the findings. Will considered removing the post, but he did not want to discard his most popular entry.

*Greatness is won
not awarded.*

GUY KAWASAKI

CLOSING THOUGHTS

- **Abraham Lincoln:** If once you forfeit the confidence of your fellow-citizens, you can never regain their respect and esteem.
- **Martha Gellhorn:** Citizenship is a tough occupation which obliges the citizen to make his own informed opinion and stand by it.
- **Robbie Sinclair:** Security is always expensive until it is not enough.
- **Ralph Nader:** There can be no daily democracy without daily citizenship.
- **Diogenes:** I am a citizen of the world.



Rick Chisholm made history when he single-handedly changed the professional Audio Visual industry by breaking all the rules and capitalised over 50% market share in Australia with very little capital, no partners, mergers or lenders and set up the first franchise operation of its kind in the world in the late 1990's and early 2000's.

As a 7x founder of companies and 30x businesses such as Innovest, AI Machine, Lightsounds, LSW, Light Emotion with revenue in excess of \$300 million and having employed more than 1,000 staff over the last 35 years. Rick is known as the Start-Up and SME Guru and is Author of a number of books including Business Success for Life. Unlike many mentors, he actually walks the talk and has a number of businesses under management in such areas as Automation, Events management, Importing, Distribution, Retailing and E-commerce.

His BIG passion is Business Education empowering Businesses Owners through knowledge and skills. Whilst Rick has experienced great success, he has also endured many failures. Rick has faced and overcome the exact same challenges you are facing now.



Tala Chisholm is an SME specialist who has owned and managed several small to medium sized businesses in the last 20 years, several of which were eventually sold. She has extensive experience in the fields of retail, franchising, licensing, dealerships, education, importing, distribution and consulting.

Her expertise lies in building and implementing customised cross-platform database and software solutions for businesses, automation, IT, web marketing, advertising, graphic design, business administration, process refinement and implementation. Her business experience ranges from bricks-and-mortar Giftware retailing to highly technical fields such as Security, CCTV, Entertainment Lighting and Audio sales, hire and installations as well as e-commerce.

Throughout her career she also trained and mentored Franchise business owners as well as internal division managers. Some areas of training included retail operations, management practices, business strategy, accounting, cash-flow, marketing, customer service and IT. She has also headed up the drafting of Operating Compliance Manuals for Franchise operations and implementation of all the elements involved.

.....
Phone: +61 2 8007 2907
E-mail: admin@innovestsme.com.au
Website: www.innovestsme.com.au