

all about computers

Teachers
Resource
Guide

> keep it safe

Security and
Storage Solutions
for Your Schools





all about computers

Teachers
Resource
Guide

The past few years have witnessed explosive growth in school technology. This is an exciting time for educators, however connectedness brings a new set of cautions and responsibilities that schools must understand and address.

CDW Government, Inc. (CDW•G) and the Discovery Channel School are committed to helping your school meet these responsibilities. We have prepared this booklet as an easy to understand overview of network security to keep your students and network safe and secure.

About CDW•G

A wholly owned subsidiary of CDW Corp., Inc. (Nasdaq: CDWC), CDW•G addresses the unique needs of the government and education markets with brand-name technology products and services. CDW•G is a leading source of technology products and services from top-name brands such as Cisco, Hewlett-Packard, IBM, Microsoft and Toshiba. For more information about CDW•G's product offerings, procurement options, service and solutions, call 1-800-863-4239 or visit the CDW•G Website at CDWG.com.

About Discovery Channel School

Discovery Channel School is a trusted name in educational media. Its classroom-focused product line includes more than 600 videos, CD-ROMs and print resources tailor-made for use in schools.

Discoveryschool.com offers free resources for teachers, students, and parents. With more than 18 million page views a month, Education Market Research ranked the site as one of the top ten most-visited education sites.

Through publishing and online businesses, numerous strategic partnerships, and industry-leading public service initiatives, Discovery Channel School reaches approximately 90,000 U.S. K-12 schools, benefiting some 35 million students each year.

> keep it safe

Security and Storage Solutions for Schools

Twenty years ago, the use of computers in schools was a heady topic. Experts offered many bold predictions about the coming world of electronic education. However, educators soon came to realize that computers were simply another tool, which by themselves were not the stuff of revolution. However today teachers are learning how to combine global access with their curricula. These networked computers with Internet access are now bringing substance to those early predictions. Although the advantages are self-evident, networks with Internet access bring a new set of responsibilities to schools. This brochure is an introduction to those responsibilities.

All computers, and especially networked computers, are like a small town bank. When families kept their own money, any house was an easy target, but the loss was small. When the bank came to town, money was centralized and the potential loss was great. Therefore the bank had to be secure. Similarly, with networked computers data is centralized and must be secure. Network security sounds intimidating, and parts of network security are highly technical – but it's important to realize that network *activities* are a human endeavor. The bulk of network security involves managing these human activities. The concepts are practical and easy to understand.

What are the characteristics of a secure network? On a secure network:

- Services are always available. When users log on, their files are available, the Internet is available, and shields against viruses, inappropriate content, and other undesirable effects are in place.
- Documents, tables, and other stored files are protected from loss or unauthorized access.
- Users are protected from abuse from other users or outsiders.
- The network cannot be used to attack, disrupt, or invade other computer users.
- The network and its services are managed to ensure the continued good will of the community that it serves.



Passwords

The main requirement for a secure network is to protect users, their files, and services. It must keep out all other unauthorized persons. Like the PIN for a bank debit card, the key to this controlled access is password authorization. At central points within networks, special computers called servers, monitor user computers (workstations). When a user enters his logon name and password at a workstation, the server compares this information with its stored lists and allows controlled access to the appropriate files and services. Here are two examples of logon name and password authorization:

Student

- Logon name = Billypa (Billy Paine, first name and first two letters of last name.)
- Password = penfuzz (Passwords will be described below.)
- Files allowed = Personal directory for storing personal documents. Class directory for sharing personal files with classmates. Teacher's directory with only write to privileges to send personal files to the teacher for grading.

Services allowed = Filtered Internet access.

Teacher

- Logon name = Clairesl (Claire Slade, first name and first two letters of last name.)
- Password = leg sponge (Passwords will be described below.)
- Files allowed = Personal directory for storing personal documents. Class directory for sharing personal files with students. Teacher's directory with *full* privileges to send and receive student files. *Full* privileges over the personal directories of students in this class so that files can be retrieved, returned, and maintained by the class teacher. Administrative directory for grade submission.
- Services allowed = Unfiltered Internet access.

As you can see, the controlling server allows different file and service access to these users based on their logon name and password. The important point here is that the only thing that keeps Billy Paine from accessing his grades or the files of his classmates is Ms Claire's password! For this reason, the foundation of a secure network is password security. Put another way, the security of a network is only as good as its password structure.

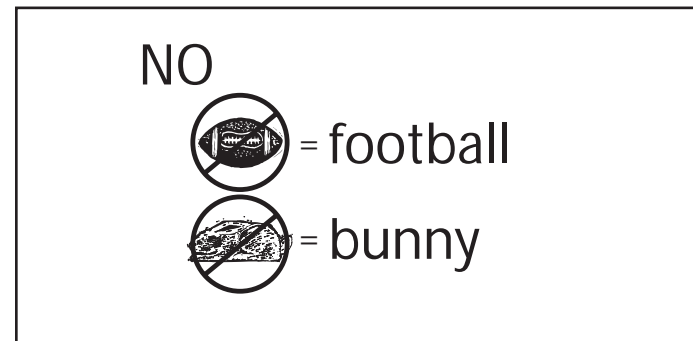
Password Structure

Good password structure begins with the system that creates passwords. There are several password weaknesses that must be avoided. The first among these is the use of a word as a password, such as "hickory". The problem is that password-cracking programs based on a dictionary are easily available to those who would attack your network. These programs simply try every word in the dictionary to see if one will work. Adding insult to injury, some of these programs use the spelling dictionary on the target computer! This threat is easily avoided by insuring that no password is also a dictionary word.

Next are passwords that are related to known features of the target user. One teacher account was compromised when students correctly guessed that the password was the name of the teacher's son. Similarly, passwords based on hobbies, favorite sports or

sports teams, girlfriends, boyfriends, pets, and so on are the first candidates of an attacker trying to guess a password.

Short passwords are easier to discover by trial and error than long ones. This is simply a statistical effect and can be avoided by network policy—passwords must contain a minimum number of characters to be valid.



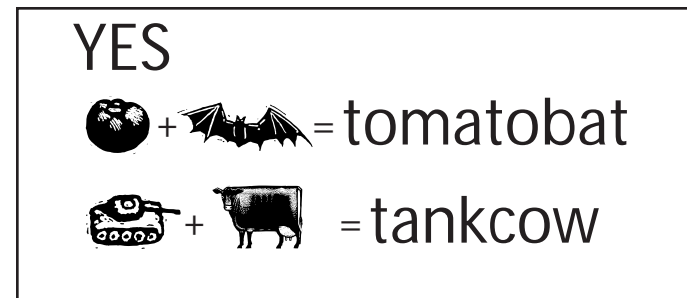
So What Makes a Highly Secure Password?

By avoiding the weaknesses above, a highly secure password can be crafted that contains a long string of random characters including numbers, punctuation marks, and upper and lower case characters. But is this the safest password?

Here is a highly secure password: e7Hnt%3to. Although this is not likely to be guessed or revealed by a dictionary cracker, this password is not safe simply because it's too hard to remember. The user is likely to write it down, perhaps where it might be found. Furthermore, because it involves keyboard shifts and special characters, typing this password is likely to be slow and therefore easier to observe. Remember, the bulk of network security is devoted to managing human activities. A secure and safe password must be reasonably easy to memorize, type, and still avoid the weaknesses above.

Here are two systems for generating passwords that are a good compromise between high security and ease of memorization and typing.

Combining two unrelated words—good for lower grades. Words such as pan and ink are unrelated and when combined to make panink, are not likely to be discovered by a dictionary cracker. The resulting word is long enough to avoid random combination guessing and in no way identifies the user.



A two-word combination lends itself to a mental image, usually strange, that is easy to visualize and easy to remember. There is no need to write it down. A password that tends to be forgotten is less secure because as a student tries vainly to enter it, there is a greater possibility for a chance observation that will compromise its secrecy. Furthermore, dealing with one or several forgotten passwords is a nuisance.

Acronyms based on lyrics, verse, or text—more secure. The passwords *wywuas*, *cmisya*, *fsasya* are very secure and cannot be guessed unless the source is known.

- *wywuas* - when you wish upon a star... (Disney)
- *cmisya* - call me ishmael. Some years ago... (Moby Dick)
- *fsasya* - four score and seven years ago... (Gettysburg Address)

This password system has the added advantage that the length of the password can be quite long. Remembering the password is best done by remembering an image associated with the source, not the letters themselves. For example, *fsasya* is easy to remember if associated with an image of Lincoln sitting at a workstation.

Passwords and Human Nature

The overwhelming majority of network abuse begins with a password-holding member of the network. This is true in the business world and is certainly true in schools. Further, these attacks do not begin with some malicious software or high-tech gadget. Rather, they involve misuse of a "loaned" password or even an over-the-shoulder glance as a user logs in.

Job number one for anyone associated with a network is to make crystal clear the responsibility of all network users to keep their passwords strictly to themselves and to protect them from discovery. You've seen how to teach students how to craft passwords that are secure and practical, but this effort has no value if users allow others to use their passwords.

Here are the main points to promote among students:

- Tell students that a malicious attack from the outside is easier if the attacker knows a legitimate logon name and password. Therefore, protecting passwords protects everyone on the network.
- Tell them that Network Administrators can track activities to a logon name and password. If someone uses their password to abuse the network, the administrators will be looking for them. They may not be responsible for the abuse, but they are responsible for allowing their password to be used by the abuser.
- Remind students that the most common method for capturing a password is to look over the user's shoulder as they log on. They should look around to insure that no one is in a position to watch as they enter their password.
- Explain why they should not undermine the discipline imposed on a fellow student. Sometimes, a student, perhaps a friend, who has been removed from the network, may plead with them for the use of their password so that he "...can finish this important assignment." They must understand that this student was removed from the network for cause. The student may express sympathy but should deny the plea. The student off the network must appeal to his teacher.
- Remind students that computer and network access is a privilege. They have a duty to protect the network and all the students and staff who use it. If they discover that a password is known, they must report it to an adult. If it is awkward, they don't have to name the students who know, but they must say that the password for logon name so-and-so is known. The sooner they tell, the sooner the network will be secure again.



However, promoting network security awareness is not limited to students. Many teachers and staff are new to network security. Some may think that these guidelines are primarily directed toward students and not appreciate their importance for all. More than one password has been found taped to faculty/staff workstations. This is especially dangerous because these users usually have access to sensitive files.

One of the hardest, but most essential, tasks is to develop a school-wide sense that there are no circumstances that justify loaning a password. You must develop procedures for forgotten passwords and other hardships and insure that users know about them. This allows users to respond to a password request with a solution that does not force a choice between good will and a security breach.

Protecting the Network

Firewalls

In connecting to the Internet, your network becomes exposed to several threats. As you would expect, some of these are external and involve viruses and other forms of harmful programs called *malware*. Malicious parties may try to access, modify, or delete stored files. Other harmful programs, called spyware, report network activity to an outside computer. A special server, called a firewall that is connected to the raw Internet connection on one side and your network servers on the other, blocks these external threats. This firewall and the software installed on it are not options and their cost must be included in the cost of the network. Firewalls and firewall software are highly technical topics and selecting the best solution requires assistance from network professionals.

Anti-virus Software

In addition to these external threats, your network is internally vulnerable to users' activities. Some students may find the challenge of bypassing security, or *cracking*, to be irresistible. But the biggest problem results from users saving and loading files onto the network using floppy disks. Most school networks are configured to allow this because it's the most convenient way for

students to take their work to and from school. However, this benign activity can also import viruses from infected home computers. Whether the source of these viruses is external or internal, the solution is the same—robust anti-virus software. To remain robust, a good anti-virus protocol includes frequent automatic updates on servers and automatic updates to workstations each time a user logs on. This also is a technical topic that requires professional assistance for selection and installation. And like the firewall, is not optional.



Security is a Must

Is there such a thing as a small network that doesn't need a firewall and anti-virus software? After all, what if an Internet connected network, perhaps small, doesn't contain any critical data? Wouldn't it be easier and cheaper to simply restore an attacked network from a backup tape? Without exception, the answer is no. Even assuming that you have made backups on a regular basis, an unprotected network can be made to be an unwitting pawn in a large-scale Internet attack. Malicious parties use special malware to scan the Internet for unprotected computers. Once discovered, this network, and others, can be used to send a torrent of messages to a targeted network. The flood of incoming messages overwhelms the targeted network, effectively removing it from the Internet. This Denial of Service (DoS) attack has become more common in recent years and some attacks have had devastating effects. The Internet is one of the most significant learning resources to come from the technology revolution, but it has a dark side. Internet security is a shared responsibility and that responsibility begins with a secure network.

Protecting Users

Students are curious and will find inappropriate Internet content faster than you can imagine unless you install filtering software on the firewall server described above. School communities vary in their sensitivity to inappropriate Internet exposure, but all communities, especially for younger students, will demand some level of filtering. There are several ways to handle Internet filtering, but selecting the best solution is another technical topic that requires the assistance of network professionals. Some states have central servers that provide Internet access to their schools. In this case, Internet filtering can be done for state schools at the state's central servers.

Although essential and generally good at what it does, Internet filtering will never be completely effective. New websites appear every day, so even the best content filters that block by website identification can never be entirely current. Filters that block by looking for key words are problematic. A filter set to block content containing the word "breast" also blocks medical sites that may be part of a health assignment.

Some websites are perfectly acceptable, but involve age-inappropriate decisions. E-commerce websites like eBay and CDNOW tempt students to make financial transactions. Beyond the legality of such under-age activities are the disputes that will inevitably



arise. This is an area that schools should avoid by promoting clear policies that ban such activities. The Internet filtering mentioned above can be set to block specific sites that offer e-commerce, but your Technology Policy Group (discussed below) should set these policies.

Hardening the Network

The most significant part of a network is the hard drives that store your data. Any other part can be swapped out and everything will return to normal. But if a hard drive is lost, all the data that it contained is lost too. At this point, you can only hope that the backup tapes are good. There is a hard disk option that greatly reduces the chance of this kind of loss called RAID—Redundant Array of Independent Disks. In a RAID array, a special controller runs several hard drives together. There are six versions of RAID for different purposes, but RAID 5 provides very high reliability. If one RAID 5 disk fails, the data is not lost. Instead, the failed disk is replaced, an array restore is performed, and the array and all of its data are back to normal.



Although RAID hard drives offer a high degree of reliability, you can still suffer data loss through other causes. Water damage caused by a leaking roof, vandalism, and file loss caused by viruses are a few of the reasons why a rigorous backup system is mandatory. Networks are complex and in spite of everyone's best efforts, sooner or later data will be lost. Network professionals talk in terms of *when* data is lost, not *if*. Preventing a failure is not a valid measure of a network; the better gauge is the ability to recover. The key to reliable recovery is a daily backup of network drives. This can be a lengthy process, so backup equipment and software is designed to run unattended late at night. Whole books have been written about network backups, but here are the main ideas:

- You will probably use a tape backup system. Insure that it has enough capacity to backup all network drives in one session. Purchase a backup tape drive that has enough capacity for future network growth.
- Insure that you have enough backup tape sets to support a rotation system that allows some tapes to contain a full backup of the network as it existed several months ago. A rotation does not require a separate tape for each day; it can be done with as few as 15 tapes.
- Keep a record of backup tape use and replace them as they reach the end of their lives.
- Insure that some tapes are stored at a remote location.

The intention of these ideas is self-evident except for the second. The reason for old backups is that some viruses are designed to remain dormant for a period of time before inflicting their damage. If such a virus were to invade your network, you might need to go back several weeks to find an uncontaminated backup tape. Your network professionals will help you set up a good rotation system with as few as 15 tapes.

Making hard drive backups is the first step in data recovery. The next step is to restore data from these tapes. More than one recovery attempt has failed because the restore process had never been tested. Backup systems should be tested from time to time by following these simple steps:

- Create a meaningless file and save it on the network.
- Delete the file after your automated backup system has made a copy of it.
- Restore the file to the network from the backup system.
- Check the restored file for integrity.

It's a good idea to have every member of your Information Technology group perform this task on a rotating basis so that all members are familiar with the process.

Cabling

The cabling that connects workstations and servers together is rarely the stuff of lunch conversations, yet it deserves careful consideration. The most common way to cable a network, Ethernet, is a shared line. All of the computers on the line listen for messages bearing their address. Before a computer sends a message, it waits until there are no other messages being transmitted. You can see that like a city street, network traffic can be slowed by congestion. Your network professionals will advise you about the installation of your cabling to reduce network congestion, but there are some things that you need to watch for.

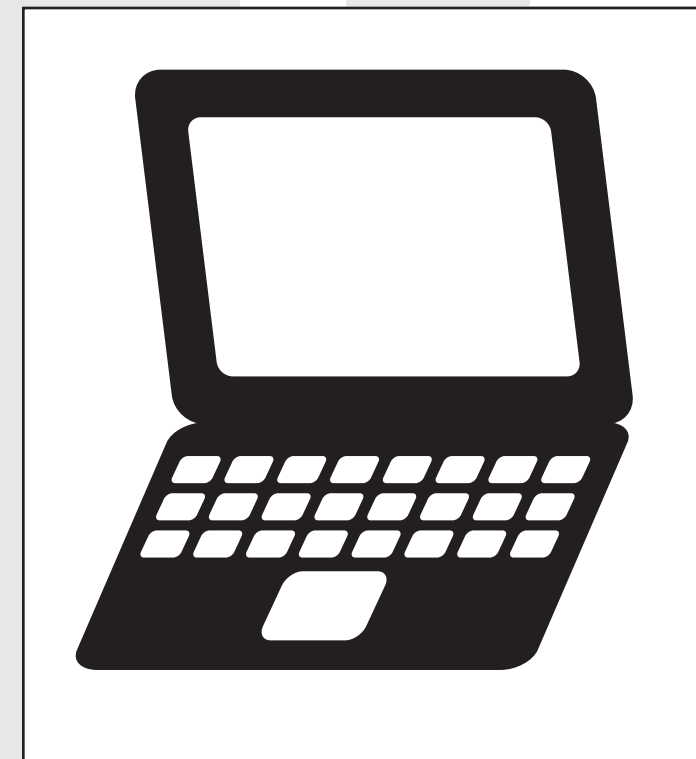
Network cabling is a radio antenna of sorts. The pairs in the cable are twisted to reduce this effect, but the cable can still pick up and transmit interference. Fluorescent light fixtures are notorious for adding noise to network cabling. This noise can be mistaken for



network traffic and cause the same network congestion described above. Radios and public address systems may hum if network cabling passes near them or their cables. You'll probably have a network company install your permanent cabling, but keep these ideas in mind when you string temporary cables.

Wiring Closets

Networks include spaces – called wiring closets – where groups of cables are brought together and connected to distribution devices. These spaces must be secure and accessible only to authorized persons. Wiring closets are vulnerable to mischief and worse. With the proliferation of inexpensive wireless routers, anyone who could slip into a wiring closet could also plug one of these devices into a switch or hub. They would then have access to the network on the trusted side of the firewall from a notebook located anywhere, even from outside of the building.



Workstation Protection

Workstations need protecting too. They can be protected from theft by locking devices that secure computers to desks or by securing the space that contains them. In addition to physical security, the programs and other settings on each workstation have to be protected from change. Curious students will change settings, download programs onto the workstation from the Internet, and in other ways alter the appearance and behavior of workstations. Other students may be unable to use such altered workstations, resulting in a call to the Information Technology group.

Usually this is not a malicious activity, and it's very difficult to control through policy. Fortunately, there are two kinds of software that work together to eliminate this problem. The first, called desktop locking software, locks the computer so that only allowed functions will operate – preventing alterations. The second, called imaging software, makes an exact copy of a hard drive. An ideal workstation is created and then imaged. The image is used to quickly restore a workstation or to bring a new computer onto the network. Both kinds of software can be controlled from a central console, making their use especially efficient.

Maintaining the Network

There are many administrative tasks that must be done everyday to keep a secure network running smoothly. The automatic logs that record server activity must be checked for abnormalities. Usually these reports are bland and similar day after day. It's easy to become casual about checking them, but this is where you will first find hints of trouble.

The backup system must be checked each morning to insure that the backup was performed successfully. If not, the cause of failure must be determined and fixed so that the next backup will be successful. The previous tape or tapes must be returned to the backup rotation and new tapes loaded for the next backup session.

Hard drives must be maintained. Servers are constantly storing data on their hard drives. The effect is similar to stuffing pages into a file cabinet. Unless someone sorts these pages out, finding a particular page will take some time. Similarly, hard drives become a great heap of scattered files that take time to retrieve. When this becomes severe, workstations become frustratingly slow. The cure for this scatter is to “defrag” (defragment) the hard drives. This process is handled by special software that, like backup software, runs at night. The defragging operation also should be confirmed each morning.

Finally, we’ve already seen that the software that keeps the network secure must be updated regularly. These updates are often automated, but it’s important to verify that this process continues to operate smoothly.



Network Groups and Policy

The behind-the-scenes administration of a network is a highly technical field. You may have faculty or staff that are expert computer users, but it’s rare that a school has the expertise needed to install and maintain a secure network. You may benefit from network professionals within the school community or you may need to contract with a network service provider. It will be vital to employ these skills in some fashion in order to form an *Information Technology Group*. A cost-effective model is to have a core of onsite members that handle the day-to-day tasks of adding new users, backing up servers, restoring workstations, and so on. Then you can contract network professionals for those tasks that require specialized skills and experience on a per-case basis to support these onsite members.

Technology Policy Group

Clearly the advantages of Internet access for schools outweigh the disadvantages, however, there are bound to be some difficulties. The best way to manage network policy is through a *Technology Policy Group* that represents teachers and parents. Some schools include students too. You may choose to establish a dedicated committee or include this responsibility within your parent organization, but the purpose in either case is to reach network policy consensus through community dialog. As long as the community feels that they have participated in these decisions, they are more likely to accept these difficulties as part of their shared responsibilities.

A significant part of maintaining a sense of community participation is to publish and promote the decisions and policies of the Technology Policy Group. Include these policies in student handbooks and with any materials distributed at the beginning of the year.

It’s important to keep the roles of the Technology Policy Group and Information Technology Group separate. There are subjective choices to be made by the Technology Policy Group and there are technical choices that must be made by the Information

Technology Group. The Technology Policy Group decides questions about the user and the use of the network, often from a list of choices provided by the Information Technology Group. The Information Technology Group implements these decisions and maintains the network. It will be far easier to reach consensus if the former decides the *what* questions and the latter answers the *how* questions. School administration must be a part of the Information Technology Group so that they are among those deciding on implementation options proposed by the technical members.

This guide was developed to help schools secure their computer network. But its significance extends beyond your school’s environment. As technology continues to advance, the ability to use networked computers will be the core of future job skills. Schools that secure their networks and develop good network behaviors among their students are providing them with valuable technical skills for tomorrow’s workforce.



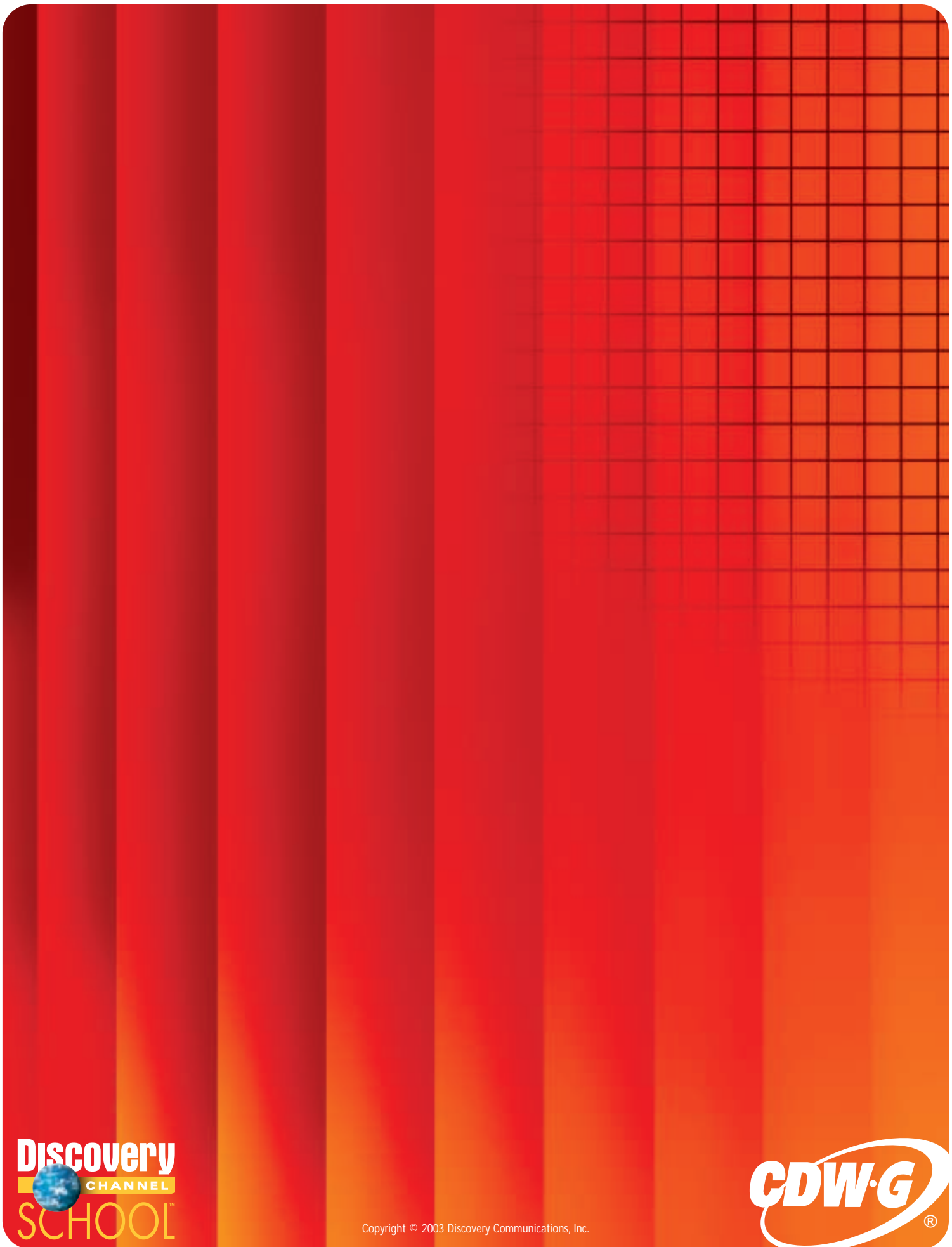
Receive a **FREE** subscription to **CDW•G's Ed Tech magazine**

CDW•G's Ed Tech provides comprehensive coverage on a wide range of topics including student privacy, security and networking, professional development, federal legislation, fiscal policy and more.

Every issue delves deeper to offer solutions and guidelines for successfully implementing information technology in today's educational environment.

Log onto CDWG.com/edtech to get your free subscription of CDW•G's Ed Tech magazine today!





Copyright © 2003 Discovery Communications, Inc.



discoveryschool.com

CDWG.com