JPPSS District

Technology Operating Policies and Procedures Manual

Document Number   JPPSS-DT-1

Created By: Dr. Mable Moore, CTO

Table of Contents

Acceptable Use of Resources Policy

This acceptable use policy governs the use of Technology Division's resources, including but not limited to, computers, laptops, hand-held mobile devices, general equipment, and networks by all persons at Jefferson Parish Public School System (JPPSS). As a user of these resources, you are responsible for reading and understanding this policy. If you have questions, please contact the JPPSS Chief Technology Officer (CTO). JPPSS encourages the use and application of Technology Division to support the instruction, and public service mission of the institution. JPPSS computers, laptops and networks provide access to resources on and off all schools within the district, as well as the ability to communicate with other users worldwide. Such open access is a privilege and requires that individual users act responsibly. Users must respect the rights of other users, respect the integrity of systems and related physical resources, and observe all relevant laws, regulations, and contractual obligations

Access to Division of Technology Resources

Careful and ethical use of computing resources is the responsibility of every user. As a user of these resources, you agree to be subject to the guidelines of the "Policy Governing Access To and Use of the JPPSS Division of Technology Resources", below. These guidelines apply to all computing and technology resources provided by JPPSS. This policy includes and expands upon those guidelines, and contains a glossary of the technical terms used in the policy (See attached glossary).

Work under approved District contracts and grants are covered under the usual internal approval processes, which serve as the requisite "prior written authorization." If you need to open a commercial account or would like more information, contact the Chief Technology Officer or the Chief Financial Officer.

For information on obtaining your own account, or how to share files or data, or forward e-mail to another user safely, please contact:

JPPSS Help Desk
349-8585

Code of Ethics for Division of Technology at JPPSS

Division of Technology facilities (computer hardware, software, networks, data and other information, etc.) are made available as shared resources intended to support and facilitate the teaching, research, and administrative functions of the students, teachers, and district employees and authorized guests. They are encouraged to use these resources to their maximum benefit in these functions. Experimentation, exploration, and learning are promoted within common sense and legal constraints.

Network and system administrators are expected to treat the contents of electronic files and network communications as private and confidential. Any inspection of

electronic files, and any action based upon such inspection, will be governed by all applicable U.S. and Louisiana laws and by District policies.

The same standards and principles of intellectual and academic freedom, as well as rights to privacy, developed for District libraries are applied to electronic material.

The same standards of intellectual and academic freedom developed for teacher and student publication in traditional media apply to publication in electronic media. Examples of these electronic materials and publishing media include, but are not limited to, electronic mail, mailing lists (Listserv), Usenet News, and World Wide Web pages.

Usefulness of the facilities depends upon the integrity of its users. These facilities may not be used in any manner prohibited by law or disallowed by licenses, contracts, or District regulations. Individuals are accountable for their own actions and all activity involving the accounts for which they have responsibility. District policies and state and federal law make certain kinds of activities involving technology abuse, civil offenses, or criminal offenses. Students, Teachers, and staff should be aware that criminal prosecution may occur if the law is violated.

NETWORK USE

The JPPSS Wide Area Network connects workstations and computers within the District. It also provides access to national and international computer networks. As you explore the JPPSS Network and the Internet, you will discover there are many advantages of network connectivity. But connectivity also requires that you understand the responsibilities of being a network user in order to protect the integrity of the system and the integrity of other users. The following policies are intended to help you use JPPSS's network responsibly and safely.

- **Use the JPPSS network appropriately**. The purpose of the JPPSS network is to support research, education, and administrative activities of students, teachers, and staff of JPPSS by providing access to computing resources and the opportunity for collaborative work. All use of the network must be consistent with this purpose.

PRINCIPLES GOVERNING USE OF COMPUTING RESOURCES

User access is granted to an individual and may not be transferred to or shared with another without explicit written authorization by the JPPSS Chief Technology Officer a designee, or the appropriate system administrator.

This principle is intended to protect the integrity, security, and privacy of your account. Sharing access with another individual undermines the security of your account, leaving it vulnerable to abuse by others. By not sharing your account, you protect against unauthorized activities on your account, for which you would be responsible. You may be charged with *a violation if someone uses your account with your permission and violates policy. Just as important, sharing or transferring access jeopardizes the security of the entire computing system because it weakens one of the "links" in the system "chain."*

Prudent and responsible use begins with common sense and includes respect for the rights and privacy of other users. For example, as a prudent and responsible user, you should:

- Not share your account with any other user.
- Protect your password by choosing it wisely, keeping it secure, and changing it regularly.
- Back up files on a regular basis to ensure the safety of important data in the event of a system failure.
- Log off your account when leaving a computer.
- Always use virus protection software.
- Store or lock technology resources, such as laptops, PDAs, etc. as appropriate to prevent theft.

Computing resources are finite and must be shared among users in an equitable manner. The user may not participate in any behavior that unreasonably interferes with the fair use of computing resources by another. During periods of peak demand, facilities may enforce guidelines to require sharing resources for the benefit of everyone.

Examples of unreasonable interference include, but are not limited to:

- Playing games for recreation and not for scholarly activities.
- Exceeding established disk space, time, or other allocations.
- Intentionally running programs that could “crash” the computer.
- Users should be advised the availability of printing resources is dependent on school policies. Please consult with your Principal.

Some examples of violations

This section of the Policy consists of a list of several activities that you cannot or should not do. While these are not all of the possible violations, there are still many more things you can do than things you can't do. This list is intended to inform you and to reinforce the principles of fair and responsible computer use that we seek to engender at the district.

A violation of these principles or any attempt to violate these principles constitutes misuse. Violations include, but are not limited to:

- ***Sharing passwords or acquiring another's password without prior written authorization from the Division of Technology or the appropriate system administrator.***

  The consequences of sharing your password can be significant for the system and for you as well. This action leaves you vulnerable to such things as impersonation by another user.

  However, even if you are not concerned about the safety of your own account and data, you have a responsibility to other users to help maintain the security of the system. Your responsibility is like that of a tenant in an apartment building. Though the tenant may not be concerned about his or her own apartment, feeling that it contains little or nothing of value, he or she still has a responsibility to the other tenants to keep the main entrance secure.

  On occasion, you may want to share files or data or e-mail with other users. For information on how to do that safely, please contact the Help Desk.

- ***Unauthorized accessing, using, copying, modifying of another’s account, or deleting of files, data, User IDs, access rights, usage records, or disk space allocations.***

  You are authorized to access, use, and copy, modify, or delete files, data, or access rights on your own account as specified in the Policy. You are not authorized to perform any of these functions on another user's account or a District system unless specifically given permission by the account holder, your job description, the CTO, a designee, or the appropriate system administrator.

> A person who finds a door to another's home unlocked does not have the right to enter the home simply because it is unsecured. Similarly, the fact that some one's account and its data are unprotected does not mean that you have the right to access it.

- ***Accessing resources for purposes other than those for which the access was originally issued, including inappropriate use of authority or special privileges***

- ***Copying or capturing licensed software for use on a system or by an individual for which the software is not authorized or licensed.***

  JPPSS subscribes to the principles expressed in the EDUCOM Guide to the Ethical and Legal Use of Software. According to U.S. Copyright Law, all intellectual works are automatically covered by copyright unless explicitly noted to the contrary. "Unauthorized copying and use of software deprives publishers and developers of a fair return for their work, increases prices, reduce the level of future support and enhancements, and can inhibit the development of new software products."

  JPPSS does not condone or authorize the illegal copying or possession of software. District students and employees are prohibited from copying software illegally and possessing illegal copies of software, whether for course, job-related, or private use. Any violations of this policy or of Copyright law are the personal responsibility of the user. JPPSS will not assume any liability for such acts. Furthermore, the Division of Technology will refuse to provide support for a user who cannot demonstrate that the software involved was obtained legally

  > *"Using Software: A Guide to the Ethical and Legal Use of Software for Members of the Academic Community" EDUCOM*
  >
  > *Link to Guide*: http://www.cni.org/docs/EDUCOM.html
  >
  > U.S. Copyright law applies to all software users. For a printed copy of the guidelines, write or call: EDUCOM, 1112 16th Street, NW, Suite 600, Washington, DC 20036, (202) 872 - 4200. If you are unsure about whether you possess legal software copies, please contact the Help Desk for more information.

- ***Use of computing resources for remote activities that are unauthorized at the remote site.***

  For example, if you are accessing another computer system using a JPPSS computing resource, you must obey that district / school's own computing guidelines. Your actions reflect upon the entire district.

- ***Causing computer failure through an intentional attempt to "crash the system," or through the intentional introduction of a program that is intended to subvert a system, such as a worm, virus, Trojan horse, or one that creates a trap door.***

You have a responsibility to other users to help maintain the security of the system. The intentional introduction of a subversive program is considered a grave offense. Taking reasonable precautions is part of your responsibility. If you think you may have accidentally introduced one of these programs, please contact your local system administrator or call the Help Desk for information on virus protection software.

- ***Intentional obscuring or forging of the date, time, physical source, logical source, or other header information of a message or transaction.***

  Header information of electronic mail, files, and printouts is an essential part of the identification and documentation of your work. Forging electronic mail or masking identification information -- for amusement, personal gain, or other reasons - is not allowed**.**

- ***Interception of transmitted information to which is not directed to you without prior written authorization from the office of the Division of Technology or the appropriate administrator.***

  You may not intercept, read, copy of otherwise monitor transmitted information sent by and between other employees within the system unless you are authorized to do so.

  In the course of system maintenance, transmissions are tracked, but not read unless unauthorized usage is detected. School system personnel can and will read transmissions by unauthorized users, to maintain the integrity and security of the computing resources for all authorized users.

- ***Failure to protect one's account from unauthorized use (e.g., leaving one's computer terminal or laptop publicly logged on but unattended)***

  When you do not protect your account from unauthorized use, you weaken the security of not only your account, but also the entire system. Keeping your password secure and attending to your account when logged on are key means of protection. You should log off your account whenever you leave your work station.

- ***Violation of priorities for use of computing resources as established by an individual facility within the JPPSS system.***

  Some JPPSS computing facilities may have no usage rules beyond those given in this Policy. However, many have established priorities for use of computing resources to ensure that scholarly activities are granted more weight than, for example, recreational game play and other non-academic pursuits. These priorities must be respected.

E-MAIL POLICY

JPPSS provides many computing and network resources for use by students, teachers, and employees. District employees are encouraged to use electronic mail (e-mail) for district-related activities to facilitate the efficient exchange of useful information. Access to e-mail is a privilege and certain responsibilities accompany that privilege. Users of e-mail are required to be ethical and responsible in their use.

Electronic mail is one of the most used and useful facilities on computer networks. To ensure maximum benefits from e-mail, a clear, defined balance between the need for open communication and the protection of the District's assets is critical.

The purpose of this policy is to encourage use of e-mail as an effective and efficient tool within the framework of the appropriate Louisiana and federal laws, District policies and rules and other necessary restrictions which apply even if they are not specifically mentioned in this policy.

Principles of Acceptable Use of Email

Access to and the responsible use of modern information resources is essential to the pursuit and achievement of excellence at JPPSS. The District encourages appropriate use of e-mail to enhance productivity through the efficient exchange of information in education, research, public service and the expression of ideas. Use of these resources must be consistent with these goals. As responsible members of the JPPSS community, everyone is expected to act in accord with the following general principles based on the acceptable law as well as common sense, common decency, and civility applied to the networked computing environment:

- **Messages sent as electronic mail should meet the same standards for distribution or display as if they were tangible documents or instruments.** Identify yourself clearly and accurately in all electronic communications. Concealing or misrepresenting your name or affiliation to dissociate yourself from responsibility for your actions is never appropriate. Alteration of the course of electronic mail, message or posting is unethical and may be grounds for discipline. One test of appropriateness would be to never 'say' anything via e-mail that you would not be willing to say directly to a person.

  Create an email signature. The technology department will help you do so if you or your supervisor does not know how.

- **Be sensitive to the inherent limitation of shared network resources**. No computer security system can absolutely prevent a determined person from accessing stored information, and JPPSS cannot guarantee the privacy or confidentiality of electronic documents.

- **Respect the rights of others**. Do not send abusive, threatening, or harassing materials. Civil discourse is at the heart of a District community free of intimidation and harassment and based upon a respect for individuals as well as a desire to learn from others. While debate on controversial issues is inevitable and essential, you may not use the District's electronic communication in a manner that violates the District's policies or applicable laws against discrimination or harassment including policy and laws against sexual harassment. The same standards or conduct expected of students, teachers and staff regarding the use of telephones, libraries, and other institutional resources apply to the use of e-mail. You will be held no less accountable for your actions in situations involving e-mail than you would be in dealing with other media.

- **Do not engage in wasteful and disruptive practices, such as creating or sending `chain letters', `broadcast' messages or unwanted material, 'flaming', or overloading a system**. This effort is consistent with existing practices governing other forms of communication on campus including telephone calls, bulletin board postings, the mass distribution of flyers and the use of intra-campus mail services;

- **The system may not be used for certain personal reasons. These reasons include, but are not necessarily limited to the following:**

    - **Political advocacy.** In accordance with Federal and State laws and the policies and procedures of the Jefferson Parish School Board, the use of public resources to promote political campaigns, referenda, or issues are prohibited. This would include transmissions, which advocate the election of particular candidates for public office at either the federal, state or local level or that advocate support of or opposition to any particular referendum proposal that will be decided by the voters during a regular or special election.

    - **Religious purposes.** This prohibits sending of messages, which contain information on religious positions or activities or that may promote religion. Those using e-mail for legitimate educational purposes should be careful to abide by the law.

    - **Others.** Other examples of inappropriate personal use of the system includes, but are not limited to, wagering, fund-raising for any purpose unless District-sanctioned, discussion or transmission of personal views regarding co-employees, supervisors or system administrators, racial, sexual or legally discriminatory harassment, discriminatory remarks.

- **E-mail and other network resources may not be used for commercial purposes or for personal financial gain.** To do so would be a violation of Louisiana state law. This does not preclude the use of e-mail to assist in the

- **Do not use access to violate Federal or State laws or the JPPSS's policies and procedures.** Conduct, which involves the use of information resources to violate a School Board policy or procedure or state or federal law, or to violate another's rights, is a serious abuse subject to limitation of your privileges and appropriate disciplinary and/or legal action. The District is not responsible for transmissions which are libelous or defamatory, but will appropriately investigate and address these unwanted transmissions with the message sender.

- **Confidential information.** By law certain data is not available to the public, such as personnel matters or non-directory education data. If e-mail is used to transmit data that must remain confidential, it should be clearly labeled as confidential. Designating messages in this manner may reduce the possibility that the recipient will disclose the data to unintended third parties, but users must take appropriate care to protect confidential data and disclose it only to persons who are legally entitled to access. Users who illegally disclose confidential material will be subject to discipline.

If unsolicited or unwanted Internet transmissions are received, or if problems or issues arise regarding JPPSS e-mail, you should contact the Help Desk.

Complaints by any user receiving electronic transmissions through any e-mail server may be submitted to the CTO or Help Desk

Anyone aware of complaints regarding the transmission of discriminatory material or any matter contrary to this policy must be reported to Human Resources. The CTO will work with the appropriate offices to investigate complaints to make a determination of its validity.

INTERNET ACCESS POLICY

It is a general policy that JPPSS District facilities used for connection to the Internet are to be used in a responsible, ethical, and legal manner in accordance with the stated objectives for Internet access and the mission of the District. Users must acknowledge their understanding of the general policy and guidelines as a condition for use of the Internet through JPPSS District. Failure to adhere to this policy and its guidelines below may result in suspension of the offender's privilege of network access by the District. Persons who make use of the resources of the District to access the Internet do so as guests of the District and are expected to conduct themselves accordingly. Conduct which adversely affects the ability of others to use the Internet or which is harmful to others will not be permitted. The District reserves the right to monitor its computing resources to protect the integrity of its computing systems, workstations, and lab facilities.

Objectives.

JPPSS provides access to the Internet in order to support the JPPSS's mission and objectives, specifically; **the Internet is used to support the following objectives:**

- Provide for the information needs of the students, teachers, and District staff and for the information needs, as deemed appropriate by the District.
- Expand the distance learning services of the District, so that the residents of the surrounding areas have access to a school without walls.
- Develop the information literacy skills of the students of the JPPSS.
- Support the lifelong learning of the community.
- Support the professional development needs of the teachers and staff of JPPSS and enhance communication between members of the District community.

Guidelines for the use of the internet by personnel

The administration has established the following guidelines:

Guideline 1. Acceptable uses of the Internet are activities which support learning and teaching. Internet users are encouraged to develop uses which meet their individual needs and which take advantage of the Internet's functions: electronic mail, conferences, bulletin boards, databases, telnet and ftp resources, etc.

Guideline 2. Unacceptable uses of the Internet include:

- Violating the rights to privacy of students and employees of the District including attempts to access another person's account, private files, or e-mail without permission of the owner.
- Use of the District's computing resources to threaten or harass others.
- Reposting personal communications without the author's prior consent.
- Copying commercial software in violation of copyright law.
- Using the Internet for any illegal activity.

- Attempts to write, produce, copy or attempt in any way to introduce any computer code designed to self-replicate, damage or otherwise hinder the performance of any computer. Any such software is commonly referred to as a computer virus.

- Attempts to alter system software or hardware configurations. Deliberate attempts to degrade or disrupt system performance will be viewed as criminal activity under applicable state and federal laws.

- Storing or printing files, materials, or messages that violate Louisiana obscenity laws.

- The display of sexually explicit materials on a District computer screen in such a manner that it can be seen by others may be a violation of the District's policies on sexual harassment.

- Playing of computer games or simulations not in support of the curriculum at JPPSS.

Guideline 3. Persons obtaining access to the Internet through JPPSS computer networks should adhere to the commonly accepted social norms of classroom behavior**.**

Guideline 4. Accounts issued to individuals are intended for the sole use of that individual. The person in whose name an account is issued is responsible at all times for its proper use. Users should change their passwords frequently.

Guideline 5. When making copies of information from the Internet, files should be downloaded to your own removable media (floppy disk, zip disk, flash disk, DVD, etc.). Files downloaded to the District's network, or hard disk drives attached to the network, are subject to deletion without notice.

Guideline 6. Access to the Internet may be limited at the District's discretion. In the event that other users are waiting to access District computing facilities, you will be asked to limit your time. Please be considerate of other users.

ACCESS BY THE ADMINISTRATION

Although the District does not routinely monitor all messages, it does have the authority, at any time, to inspect the contents of any District equipment, files, or mail on its system for any legitimate business, legal or disciplinary purpose.

- **Reasons for review.** These include, but are not limited to: reasonable suspicion of a violation of a rule or law or District policy; investigation of system problems; litigation or anticipated litigation; or a need to perform work when an employee is not available.

- **Public information.** Employee users of the District's e-mail system must understand that communications created, received or backed-up on the system may be considered to be public documents and thus, may be subject to requests for public disclosure. Employees should bear in mind that this may apply even to e-mails that contain, for example, personal feelings or remarks.

INVESTIGATION AND REVIEW OF VIOLATIONS

When the Chief Technology Officer, a designee, or the appropriate system administrator has reason to believe that a violation may have occurred, he or she may initiate an investigation and/or limit or suspend computing privileges for the individual(s) involved, pending further investigation. Human Resources will be notified of the alleged violations and work with the technology staff to investigate the matter. If a violation of any Federal or State laws or Jefferson Parish Public School policies and procedures occur, all JPSB policies and procedures regarding the disciplining of personnel will be applied.

Investigating officials will examine charges of violations with due respect for both individual privacy and the security of other users.

RESPONSE TO VIOLATIONS

Violation of this policy will result in action by the system. Violations of Louisiana statutes dealing with unlawful access or use of a computer may be referred to the police for investigation and/or prosecution. Similarly, violations of *18 U.S.C. Sec. 1030* (Federal laws dealing with unlawful access or use of a computer) may be referred to the Federal Bureau of Investigation).

Sanctions for violation of these state and federal laws may result in fines and/or jail.

JPPSS PERSONNEL ACTIONS

Personnel actions for the misuse of technology resources are imposed under the policies and procedures of the Jefferson Parish School Board and may include, but are not limited to, restriction or revocation of access rights, reimbursement to JPPSS for the computing and personnel charges incurred in detecting and proving the violation of these rules, as well as from the violation itself, suspension and termination.

Reimbursement may include compensation for staff work time related to the violation and for archiving information related to the incident.

GOVERNING LAW

In addition to District policy, unauthorized access to computer facilities, software and licensed software is the subject of both Federal and Louisiana State Law.

JPPSS retains the right to revoke, amend, or change the provisions of this policy. The system administrator will establish more detailed guidelines as needed, for specific computer systems and networks. These guidelines will cover such issues as allowing connect time and disc space, handling of irretrievable mail, responsibility for account approval and other items related to administering the system.

GLOSSARY

Access right - permission to use a JPPSS computing resource according to appropriate limitations, controls, and guidelines.

Blogging- sometimes referred to as a web log consisting of a collection of work of many authors. A Blog is a website where entries are edited and commonly displayed in reverse chronological order. The term "Blog" can also be used as a verb, meaning *to maintain or add content to a blog.*

Commercial purpose - a goal or end involving the buying and/or selling of goods or services for the purpose of making a profit.

Computing resource - any computing/network equipment, facility, or service made available to users by the JPPSS District.

Data - a representation of facts, concepts, or instructions suitable for communication, interpretation, or processing by human or automatic means.

Digital immigrant - an individual who grew up without digital technology and adopted it later.

Digital native - a person who has grown up with digital technology such as computers, the Internet, mobile phones and MP3.

Disk space allocation - the amount of disk storage space assigned to a particular user by District Network Services or the appropriate system administrator.

Fair use - use of computing resources in accordance with this policy and with the rules of an individual JPPSS facility; use of computing resources so as not to unreasonably interfere with the use of the same resources by others.

File - a collection of data treated as a unit.

iPod - A small portable music player designed by Apple.   Users can transfer songs to their iPod with their computer using iTunes the iPod software.

Inappropriate use of authority or special privilege - use of one's access right(s) or position of authority in a manner that violates the rules for use of those privileges as specified by the CTO, a designee, or the appropriate system administrator.

Mashup - a web application that combines data from more than one source into a single integrated tool; an example is the use of cartographic data from *Google Maps* to add location information to real-estate data, thereby creating a new and distinct web service that was not originally provided by either source.

Password - a string of characters that a user must supply to meet security requirements before gaining access to a particular computing resource.

Phishing - a process in which someone claiming to be from a legitimate business or corporation sends an e-mail directing the recipient to visit a Web site where he or she is asked to update personal information, such as passwords, social security, banking account numbers, etc. This site is bogus, setup to look like the legitimate site, but its sole purpose is to gain your confidential info. No legitimate business will operate in this manner.

Pod Casting - allows subscribers to subscribe to a set of feeds to view syndicated Web site content. With pod casting however, you have a set of subscriptions that are checked regularly for updates and instead of reading the feeds on your computer screen you listen to the new content on your iPod or portable device.

Prudent and responsible use - use of computing resources in a manner that promotes the efficient use and security of one's own access right(s), the access rights of other users, and JPPSS computing resources.

Remote activity - any computing action or behavior that accesses remote site facilities via a JPPSS computing resource.

Remote site - any computing/network equipment, facility, or service not part of, but connected with, JPPSS computing resources via a communications network.

Spam - unsolicited electronic junk mail usually advertising some product. This email is generally sent in mass quantities to email addresses that have been harvested.

System administrator - any individual authorized by the CTO, or a designee to administer a particular computing hardware system and/or its system software.

Transmission - the transfer of a signal, message, or other form of intelligence from one location to another.

Trojan Horse - a program that secretly piggybacks on another download. It usually appears as a useful freebee utility but once it has been run or executed it may assist in downloading other malicious programs.

Unauthorized act - with the exception of computing actions or behaviors permitted in this policy, any such act performed without the explicit permission of the Chief Technology Officer, a designee, or the appropriate system administrator.

Usage record - information or data indicating the level of usage of computing resources by a particular user.

User - any individual -- whether student, teachers, staff, or individual external to JPPSS -- who uses JPPSS computing resources.

User ID - a character string that uniquely identifies a particular user to a JPPSS computing resource.

Web 2.0 - an umbrella term for the second wave of the World Wide Web, which refers to two major paradigm shifts. The one most often touted is "user-generated content," which relates more to individuals. The second, which is equally significant, but more related to business. User-generated content, comprised of blogs, wikis and social networking sites, such as MySpace and Friendster, let everyone have their say on anything and publish it to the world at large. As Web applications become more sophisticated, people can easily develop elaborate personal Web pages, create a blog, and upload their own opinions, using audio and video.

Wiki - a collaborative Web site which comprises the perpetual collective work of many authors. Similar to a blog in structure and logic, a wiki allows anyone to edit, delete or modify content that has been placed on the Web site using a browser interface. Wiki" is also a Hawaiian word for fast.

Worm - a destructive program that spreads through e-mail by using its own e-mail engine. Worms find e-mail addresses on your hard drive and send copies of themselves to each address in your email address book.

Virus - a malicious program that is spread by attaching itself to a program or file so it can travel from one computer to another. Damage can range from irritating messages to destruction of everything on your hard drive.

Vod Casting - a term used to describe the online delivery of video on demand digitally using a video clip to a portable device (iPod).

Zombies - unprotected computers that fall victim to spammers who pirate the machines to send their e-mail for them, making it very difficult to apprehend the spammers.