

St. Patrick's College Ballarat

Laptop Handbook



ST. PATRICK'S COLLEGE BALLARAT
1431 STURT ST BALLARAT, VICTORIA 3350
+61 03 53 311 688
WWW.STPATS.VIC.EDU.AU



Handbook Contents

Handbook Contents	2
1. Introduction.....	3
2. Consequences of Improper Use	4
3. Using the Laptop.....	5
3.1 Wi-Fi and Internet connectivity	5
3.2 File Management and Backing-Up work	5
3.3 Software Center.....	5
3.4 Microsoft Store	5
3.5 Office 365	5
3.6 Printing.....	5
3.7 e-Textbooks.....	6
3.8 Supporting your son with their laptop.....	6
3.9 Being prepared for school	6
4. Caring for the Laptop.....	7
4.1 General Care of laptop	7
4.2 Screen.....	7
4.3 Batteries	7
4.4 Support with laptop issues	7
5. Digital Safety and Citizenship	8
5.1 Looking after yourself.....	8
5.2 Looking after others	8
5.3 Looking after property	8
6. Dealing with inappropriate communications or abuse online.....	9
7. Insurance	10
8. Security	11
9. Agreement Update	12
Appendix A - Responsible ICT Usage.....	13
Appendix B - Protocols for using my ICT device responsibly for learning	14
Appendix C - Glossary.....	15

1. Introduction

In line with the College's mission of '*Raising fine boys to the status of great men*', the vision for eLearning is:

To provide technology-enriched learning opportunities that enable students to achieve high quality learning outcomes, preparing them for further education, training and to live and work in a digital world.

St Patrick's College aims to improve each boy's ability to thrive and think critically in an information rich world. This requires that technology be seamlessly accessible and integrated throughout the curriculum. Our learning programmes are constantly being reviewed and refined to meet the opportunities that new technologies will provide for your son.

Our eLearning vision will be fulfilled through the explicit use of digital pedagogy. Digital pedagogy is a way of working and learning with ICT to facilitate quality learning experiences for 21st century digital learners. It is defined as the convergence of ICT tools, technical skills, pedagogical practices and understanding of curriculum design appropriate for digital learners. Used effectively, the appropriate and relevant choice of digital pedagogy:

- Supports, enhances, enables and transforms learning and teaching to provide diverse and flexible learning opportunities for a digital generation;
- Provides the tool for engaging students in actively constructing and applying rich learning in purposeful and meaningful ways;
- Enhances opportunities for authentic, contextualised assessment that supports learning in a digital context; and
- Requires teachers to understand how teaching practices that are already commonly used in the classroom can be redesigned to incorporate digital tools and technologies to enhance and extend the learning experience for students.

St Patrick's has embraced a 1:1 laptop program for all students to enhance teaching and learning across the school. Students at the college also share specialist and general-purpose desktop computers in a lab or pod configuration and have access to other technology.

2. Consequences of Improper Use

When connected to the network, the College will filter and monitor email, web traffic and content accessed by students to ensure appropriate usage. Any breach of the protocols will be recorded, and the student may be subject to the following consequences in line with the colleges behavioral support protocols:

- Warning
- Incident added to student's Behavioral Tracking record
- Informing parents/guardians
- Completing community service
- Lunchtime or after school detention
- Suspension
- Device restrictions
- Remove all non-educational apps and software (games, social media etc)
- Limiting student access to device
- Resetting the device
- Incurring the cost of replacement of equipment
- Return of the device to the College
- Legal action

3. Using the Laptop

3.1 Wi-Fi and Internet connectivity

Whilst at school students will be provided with access to the Internet through the colleges networking infrastructure and Wi-Fi setup. Whilst using the Internet students need to be aware of the Responsible ICT Usage document. Students should not connect to any unauthorized or unknown SSID Wi-Fi signals including portable Wi-Fi modems or tethering to mobile phones.

At home students are permitted to connect their device to their home Internet and networking infrastructure but are still reminded to abide by the college's Responsible ICT Usage document as their device is connected to St. Patrick's College.

Students should be aware of the terms Malware, Phishing, Spyware, Viruses, Worms and Trojans. Access to the Internet and actions whilst online can compromise your laptop and your personal identity. Measures are taken by the colleges ICT department to protect students against malicious activity, but students are reminded that their actions do have consequences and that they should listen to advice given about their online use.

3.2 File Management and Backing-Up work

Microsoft OneDrive is the default storage system for students when saving files, documents and digital work. Students should be aware that content stored here is also accessible on different devices and online. Content stored in OneDrive is automatically backed up.

Students should use meaning names for their files and folders to keep work organised within their OneDrive. It is recommended that students have folders for the year level they are in followed by the subject they are undertaking. Files naming should be descriptive of the topic and task that a student is undertaking.



Students should regularly save their work as they are undertaking a task and they should close files when they are finished working on them. Losing a document due to mismanagement and naming is not an appropriate excuse for not submitting work. Students will be penalized as usual for late submission of work.

3.3 Software Center

The only authorised means for students to install software on their device is through the Software Center application on a student's device. The applications available in Software Center are fully licensed to the college and available for students to use on their device. Students are asked to be mindful when installing applications and software for their classroom needs and be fully prepared for lessons using any required applications. Students should not undertake the installing of software during class time as this process may require restarting of the laptop and distract students from undertaking lesson objectives.

3.4 Microsoft Store

Students are permitted to install verified apps through the Microsoft app store that appear in the connected St. Patrick's College account.

3.5 Office 365

The default application for students when word processing, notetaking, presentations and spreadsheets is Microsoft Office. Studies have identified Microsoft Office as a core skill that students will use in the workplace.

3.6 Printing

Students are permitted to install school printers on their device through the SIMON Intranet portal <https://intranet.stpats.vic.edu.au/> and will be charged for this printing at rates depending on the type of copy. Students can connect and install modern home printers on their laptop through the add printers and scanners option. If students require

support to install a home printer, they can seek assistance from the ICT department.

3.7 e-Textbooks (is it all Year levels now?)

Students in years 7 – 10 will be using e-Textbooks on their device for classwork and learning. The software for this will be installed on devices for students and will also be available through Software Center. Students will be given access to all the textbooks and resources they need of this type. Any additional resources for a class will be outlined on the college's booklist. Students should have all of the textbooks required for their subjects downloaded and ready for classroom use as directed by their teachers.

3.8 Supporting your son with their laptop

- Maintain an open, honest dialogue about online activities both academic and social. Discuss things such as standards, values, expectations and consequences both for themselves and others
- Raise any concerns about your son's use of the laptop with the College to discuss appropriate strategies and solutions
- Become familiar with current technologies used by your son and take an interest in their online life
- Assist to protect personal information
- The eSafety commissioner website has various resources and information for parents and students regarding the use of devices and online software. Parents can visit the website at <https://www.esafety.gov.au/>
- It is recommended that devices connected to the Internet be used in a family common room where parents can keep tabs on both online activity and use of the device
- Total screen time of the laptop should be negotiated between parents and their son and monitored
- Ensure that no inappropriate material is loaded onto the laptop and brought to school.
- School related use of the laptop should be kept within the suggested homework time i.e.

Year 7 & 8:	1 – 1.5 hours per night (5 nights per week)	1 – 1.5 hours per weekend
Year 9 & 10:	1.5 - 2 hours per night (5 nights per week)	1.5 – 2 hours per weekend
Year 11:	2 – 3 hours per night (5 nights per week)	2 – 3 hours per weekend
Year 12:	3 hours per night (5 nights a week)	3 hours per weekend

3.9 Being prepared for school

- Students should bring to school a fully charged laptop device each day and charge their device overnight.
- Any software required for school should be installed in preparation for classes.

4. Caring for the Laptop

4.1 General Care of laptop

- Avoid leaving the laptop in heat above 35°C or below 0°C for extended periods of time;
- Avoid exposing the laptop to water, rain, liquids or extremely humid conditions;
- Do not attempt to dry laptops with an external heat source such as a hairdryer or hand dryer. If a device is exposed to liquids turn it off immediately and take it to the schools ICT department for review;
- Avoid leaving the laptop in a vehicle. If necessary, ensure the device is secured in the boot and out of sight;
- Do not put anything into port connections apart from intended peripherals.
- When not in use, or moving between classrooms, students must keep the laptop inside the College approved protective bag.
- Avoid using or leaving the laptop in inappropriate environments. E.g., the beach, swimming pools, trampolines, in the vicinity of pets (dogs, cats, horses etc.), the snow or on the floor;
- Using the laptop outdoors should be avoided;
- Do not use the laptop while walking or running;
- Do not deface the laptop or its case with stickers or by drawing on the device with a pen or pencil.
- Do not remove keys, or protective pads from the device
- Always close the laptop for transport with the keyboard touching the screen. Do not pack the device away or transport in Tablet mode.
- Always shutdown the device for transport. Do not leave the laptop in hibernation mode or full power mode.
- Do not cover the laptops ventilation and cooling systems when using the device
- Do not walk around holding the device in potentially damaging ways. i.e. holding the device by the screen or holding it low by your knees.

4.2 Screen

- Avoid knocking or dropping device on hard surfaces or putting force on the screen. This includes textbooks or pencil cases;
- Clean often with a soft, slightly damp, lint-free cloth so long-term smudges don't affect the coating;
- Don't use window cleaners, glass cleaners, aerosol sprays, abrasives, or alcohol;
- Do not close the laptop lid with anything between the screen and the keyboard

4.3 Batteries

- Laptop batteries are rechargeable, but they will eventually wear out. They will last longer if you
 - Use battery saver mode for times of heavy use and keep battery saver mode at or above 20%
 - Install updates on your device that will improve and enhance battery life;
 - Make sure you are using the supplied laptop charger
 - Ensure your laptop is fully charged for a day's use at school

4.4 Support with laptop issues

If students have an issue with their laptop whilst at school, they will need to:

- Seek assistance from their Pastoral Care teacher, subject teachers and the ICT Department;
- If there is a hardware issue or the teacher is unable to resolve the issue, seek technical support from the ICT Department.

5. Digital Safety and Citizenship

A good citizen is someone who upholds and respects the laws of their country, but also acts in an appropriate way. Good citizens respect moral and ethical guidelines and behaviours. They show care and concern for themselves, their neighbours and other members of their communities. A good citizen respects other people's property, and expects others to do the same for them.

A good digital citizen applies the same rules to the cyber-world. A good digital citizen is a person who obeys the legal rules about using digital technologies, and acts with respect and care for themselves, others and property. In return, they expect the same respect to be shown to them. There are three key parts to digital citizenship - looking after yourself, other people and property.

5.1 Looking after yourself

- Choosing online names that are suitable and respectful;
- Only inviting people you actually know in the real world to be your friends in the online world;
- Only visiting sites that are appropriate and respect the rules that websites have about age. Some sites are only for adults. If you wouldn't feel comfortable showing the website to your parents or grandparents then it is inappropriate;
- Setting your privacy settings so that only the people you know can see you and your personal information;
- Using passwords that are hard to guess and keep these secret;
- Only putting information online that is appropriate and posting pictures that are suitable. Not everyone seeing your profile or pictures will be friendly;
- Always reporting anything that happens online that makes you feel uncomfortable or unhappy;
- Talking to trusted adults, like your parents and teachers, about your online experiences. This includes both the good and the bad experiences.

5.2 Looking after others

- Show you care by not sending hurtful or inflammatory messages to other people;
- Show you care by not sending inappropriate messages, videos or images or links to other people that contain obscene, disgusting or adult language or themes;
- By not getting involved in conversations that are unkind, mean or bullying;
- By reporting any conversations you see that are unkind, mean or bullying. Imagine if the things being written were about you. If you would find them offensive then they are inappropriate;
- Some websites are disrespectful because they show people behaving inappropriately or illegally – or are racist, bigoted or unkind. Show your respect for others by avoiding these sites. If you visit one by accident, close it and tell your teacher or an adult;
- Show respect for other's privacy by not trying to get into their online spaces without invitation, by not stalking them or copying their pictures.

5.3 Looking after property

- By not stealing other people's property. It's easy to download music, games and movies, but piracy (downloading media that you have not bought) is just the name given to stealing online;
- By not sharing the music, movies, games and other software that you own with other people;
- By checking that the information you are using is correct. Anyone can say anything on the web, so you need to check that the research is correct by using reliable sites. When in doubt ask your teacher or your parents; and
- By looking after other people's websites, acting appropriately when visiting them, not making changes or vandalising them, and reporting any damage that you find.

6. Dealing with inappropriate communications or abuse online

Abuse online can take various forms including but not limited to cyberbullying, illegal and harmful content and image-based abuse. If students are subject to this form of online behavior they need to be aware of what they can do.

- Tell someone you trust – a parent, teacher, year level coordinator or other adult;
- Avoid responding to the online behaviour; leave the site or conversation;
- Collect evidence – do not delete any offending material or take screen shots of any offending material;
- Block the contact or remove them from your list;
- Check that your profile settings are private; and
- Avoid opening messages from people you don't know.
- Review the protocols and procedures on the eSafety Commissioner website.

Students and parents are encouraged to be aware of the content covered on the eSafety Commissioner website concerning safety online. The website can be accessed via <https://esafety.gov.au/>

Online content for further information:

- <http://www.staysmartonline.gov.au>
- <https://www.esafety.gov.au/parents>
- <https://twitter.com/esafetyoffice>
- <https://www.facebook.com/eSafetyOffice>

7. Insurance

- 7.1 You must immediately inform the College if the Device is lost, stolen or accidentally damaged. Where the Device is stolen, lost or damaged all relevant circumstances and other information required must be reported by **you** to the College. The St Patricks ICT Department support centre will provide you with the appropriate forms and advise You of what action is required.
- 7.1.1 Where the device is stolen You must notify the Police of the incident and provide the College with the report prepared by the Police recording the incident.
- 7.1.2 Where the device is lost whilst the student is on public transport You must provide to the College a copy of correspondence with the relevant transport authority showing best endeavours by you to recover the device.
- 7.2 The College will insure the Device for the period from the date of this agreement which is specified in the definitions of this agreement. An insurance premium is included in the St Patricks College Laptop Fees.
- 7.3 Should an insurance claim be made in respect of the Device and be accepted You will be charged an excess of \$200 per claim and be provided a free replacement Device until the Device is repaired or replaced. The student's responsibility for the replacement device will be the same as those contained in the original Laptop Agreement.
- 7.4 If a claim is accepted the excess of \$200 will be paid by the College and charged to your fee account prior to the release of the repaired device or the provision of a replacement back to the College for supply to the student.
- 7.5 If a claim is not accepted under insurance and if any repair work is not covered by the device warranty, **you** will have to meet the College's cost in repairing or replacing the Device. We will notify you of the estimated cost of the repairs and the repair work or replacement and will then arrange for the Device to be repaired or replaced, where appropriate. You will be charged for the repair costs (parts and labour) or replacement cost as part of the student's school fee account. The Student will be provided with a free replacement Device until the Device is repaired or replaced and once all documentation and approvals for repairs or replacement have been made by **you**. Please note damage to loan devices will require devices to be repaired.

WHAT ISN'T COVERED.

You acknowledge that you cannot claim anything for:

- 7.5.1 The first \$200.00 of each and every claim
- 7.5.2 Electrical or mechanical malfunction or derangement
- 7.5.3 Scratches and normal wear and tear
- 7.5.4 Malicious damage by the student
- 7.5.5 Loss or damage occurring while the laptop is being transported in any aircraft or watercraft unless the laptop is carried as personal baggage
- 7.5.6 Loss of or damage to software of any sort
- 7.5.7 Peripheral items that come with the device namely the stylus pen, power cord.
- 7.6 Where damage to the device is determined to be under warranty the cost to you is nil.
- 7.7 Where a student on leaving the College elects to return the device the ICT Department will assess the quality of the device. Where the ICT Department assesses that damage (if any) exceeds ordinary wear and tear the College reserves the right to charge the excess of \$200 on the student's final fee account.

8. Security

To be read in conjunction with section 7

Students must ensure the safety of their laptop at all times. They must:

- Not leave their school bags unattended when they are transporting the laptop to and from the College;
- When not in use at school, always secure their laptop in their personal locked locker;
- Leave their laptop secured in their locker whilst off-campus (school excursions, Phys Ed classes, instrument sessions, sports activities, etc);
- Not swap their laptop with another student or any other person. Parents will be responsible for the full replacement cost should a student not be able to return the laptop that was initially booked out to them;
- Not leave their laptop unattended;
- Not leave their laptop in a motor vehicle; and
- Not use their laptop in an unsafe or dangerous manner.

Should the laptop be stolen as a result of or failure of any of the above, it will be the responsibility of the parent/guardian to pay for a replacement in accordance with clause 8 of this Agreement.

9. Agreement Update

This Agreement will be updated as necessary. All attempts will be made to adhere to the above mentioned Agreement, but particular circumstances (not limited to, but including technological advancements) may require the College to review and depart from the stated Agreement.



Appendix A - Responsible ICT Usage

St Patrick's College is committed to the provision of high quality, relevant educational experiences for all its users. Due to the dynamic and interactive nature of Information Communication Technologies (ICT), usage rules are required to ensure ICT equipment and online services are accessed appropriately. When accessing College ICT equipment, whether at school, home or elsewhere, and when using their own ICT Devices at school, students agree to follow all guidelines as stated below. The term 'ICT Equipment' refers to Desktop Computers, Laptops, iPads, iPods, Tablets, Mobile Phones and similar devices.

1. I will always use ICT equipment in an appropriate, ethical, legal and responsible manner and only as directed by a staff member. I will not intentionally create, access, search for, upload, execute, print or send inappropriate, offensive, violent, pornographic, subversive or dangerous material at any time from any ICT equipment in the College.
2. I will not install applications that would be deemed inappropriate or offensive or have a rating unsuitable for my age group. This includes, but is not limited to applications that contain: cartoon/fantasy violence, realistic violence, mature/suggestive themes, horror/fear themes or profanity.
3. I will respect the school security systems (including antivirus, web filtering and monitoring) and not attempt to bypass them, hack, deliberately cause disruption to the College network to or gain unauthorised access. This includes but not limited to using a VPN (Virtual Private Network).
4. I will only access the Internet through the College WiFi system. I will not hotspot or tether my ICT Device to another device whilst at school.
5. I will not make deliberate attempts to destroy data by hacking or spreading viruses. I will not install or use software which is not licensed or approved by the College.
6. I will not use the College computers or ICT devices for transferring or downloading games, files, programs or music other than those approved by the College. In addition, users may not introduce games, files, or any banned programs to the College system via any external device or by email.
7. I will not jail break my ICT device. This means I will not remove restrictions imposed by the manufacturer or operator.
8. I will not hide files or applications inside folders. Files their location and use of my device will be completely transparent at all times.
9. I will treat all College ICT resources with respect and not intentionally interfere with them in any way.
10. I will have nothing to do with any material, email, communication, or activity which might cause hurt to others or myself (including but not limited to bullying, embarrassing, abusing, making false or inaccurate statements, or harassing).
11. I will not use my ICT Device to take photographs, recordings and videos of other students or staff without their express prior permission or knowledge. I will not use or distribute any such images for any purpose, in soft or hard copy.
12. I will only use the College email system using the College domain for all school related correspondence.
13. I will be careful about giving out any personal information (including photos) online about myself *or any other person*.
14. I will acknowledge the author or publisher of information from the Internet and other digital sources and will not claim the work as my own (plagiarism). Users shall observe all copyright laws when using material from the Internet, including those relating to computer software and format shifting.
15. I will not attempt to contact friends or teachers through social networking sites. I will not comment on anyone in a derogatory way online.
16. When emailing teachers directly I recognise that teachers will only respond in a timeframe that is reasonable and usually during working hours.

Appendix B - Protocols for using my ICT device responsibly for learning

These protocols are to be followed in conjunction with the St Patrick's Responsible ICT Usage Guidelines

Protocol 1: Classroom Use

- At the start and end of class, your ICT Device will be stored inside the sleeve/bag.
- Only use your ICT Device to access applications and websites when instructed to do so by a teacher.
- Your ICT Device is not to be used for music or video unless your teacher directs you to as a part of a lesson.
- Do not use your ICT Device to deliberately disrupt the learning in the classroom.
- The audio on your device is to be left on mute. Headphones are to be used when audio is required.
- Only use your ICT Device for school related purposes. You are not to access any personal content or websites during class time.
- Ensure that all programs open on your ICT Device are closed at the end of each lesson. This will help with battery life and it minimise distractions to keep you focussed on classroom tasks.
- When a teacher instructs, close the ICT Device cover or lid immediately.

Protocol 2: Personal Use

- Your device can be used for personal content, but this should not be accessed in class. Only use your ICT Device for school related purposes, during class and study sessions.
- Ensure that personal content stored on your ICT Device is appropriate at all times and understand that storage space for school related content is a priority. This includes wallpaper and language in accordance with points 1/2 of the St Patrick's ICT Responsible Use Guidelines document.

Protocol 3: Security of ICT Device / Account

- Use a complex passcode/password to protect against unauthorised use by others.
- Keep your login account details to yourself. You are responsible for any action carried out under your login username.
- Students are not to access any ICT Device using another student's or staff member's username and password.
- Do not install unauthorised software which may compromise security

Protocol 4: Charging my ICT Device

- Ensure your ICT Device is charged overnight for the next school day.
- Ensure you have enough battery life in your ICT Device to last the entire school day.

Protocol 5: Looking after my device

- Your ICT Device is to be secured in the College approved protective bag
- If the bag becomes damaged or lost, then it is your responsibility to replace it by buying a new one from the College Shop.
- The protective bag provided is not to be defaced.
- When not in use in class, store your ICT Device locked in your locker. This includes school excursion, PE classes, instrument sessions, sports activities (unless specifically requested by a staff member).
- Take care of your ICT Device, especially when in your school bag, travelling to and from the College.
- When travelling to and from school and between classes, your ICT Device will always be inside the bag provided. This also includes before school, recess, lunchtime or afterschool.

Appendix C - Glossary

Appropriate Behaviour

Acting in a way that is understanding and respectful of College ICT expectations and guidelines as documented.

Authorised

Have permission or approval.

Back up

Make a copy of your files from which a restore could be made if the original files are lost.

Black List

A list that contains the names of apps and software that are not to be installed on a school device.

Breach

Breaking or failing to observe a rule or code of conduct.

College domain email

The St. Patrick's College domain is @stpats.vic.edu.au

Compliant

To agree with or obey rules.

Derogatory

Unkind, disparaging, belittling, offensive or disrespectful comment.

Devices

Is inclusive of but not limited to PCs, laptops, tablets storage equipment (e.g. USB or memory sticks), CDs, DVDs, multimedia players (e.g. iPods), cameras, mobile phones, gaming consoles, and any other technologies that perform similar functions.

Ethical

Being in accordance with the rules or standards for right conduct or practice.

Format shifting

The conversion of media files from one format into another. E.g., converting an Adobe PDF file into a Microsoft Word document file.

Hacking

In the computer security context, a hacker is someone who seeks and exploits weaknesses in a computer system or computer network.

ICT

Is inclusive of the school's network cabling and all data and **devices** (outlined in definition above) attached to the network or stand alone. ICT also includes personal or non-school **devices** used on school premises.

Inappropriate

Refers to any malicious software, illegal material, or communication involving sex, racism, cruelty, or violence transmitted or stored which may have a negative effect on others or is incompatible with the school values.

Jail Break

This is the process of removing the limitations imposed by the manufacturer or operator.

Login/Login Account

A means of accessing the school's network using a College allocated username and password.

Personal Information

Is information including but not limited to name, address, email address, phone numbers, and photos.

Plagiarise

Making someone else's work or ideas and passing them off as your own.

Mute

Deaden or muffle the sound of the device.

Malware

Malware is an umbrella term used to refer to a variety of forms of hostile or intrusive software, including computer viruses, worms, trojan horses, ransomware, spyware, adware, scareware, and other malicious programs. It can take the form of executable code, scripts, active content, and other software.

Operating System

Is system software that manages computer hardware and software resources and provides common services for computer programs.

SSID

A connection to a wireless network

School Security Systems

Systems implemented to protect the school's ICT and users from viruses, (e.g. Firewall, Antivirus).

Social networking

An online service platform that facilitates the building of social networks or relations. E.g., Facebook, Twitter, Google+, Snapchat and others.

Spyware

Software that enables a user to obtain covert information about another's computer activities by transmitting data covertly from their hard drive.

Subversive

Disruptive, troublemaking, inflammatory.

Tether

Use (a smartphone) in order to connect a computer or other device to the Internet.

Trojan

Malicious computer program which misrepresents itself to appear useful, routine, or interesting in order to persuade a victim to install it.

Virus

A computer virus is a malware program that, when executed, replicates by inserting copies of itself (possibly modified) into other computer programs, data files, or the boot sector of the hard drive.

VPN

Virtual Private Network

Worm

A computer worm is a standalone malware computer program that replicates itself in order to spread to other computers. Often, it uses a computer network to spread itself, relying on security failures on the target computer to access it. Unlike a computer virus, it does not need to attach itself to an existing program.