PATERSON PUBLIC SCHOOLS
Preparing All Children for College and Career

Department of Technology

Helpdesk: 973 321-0905 Fax: 973 321-0901
helpdesk@paterson.k12.nj.us

Password Override Form

(Required to override blocked sites)

Requestor Name:	
Title:	
Department/School:	
Tel/Ext No.:	
User ID:	
Fax:	

Disclaimer

This service is to be used for educational and work related reasons. The override password is to be used by the user stated above. All use of the filter override password must be compliant with The Children's Internet Protection Act (CIPA). Any not permitted access caused by the passing of the password to a user not stated on the form may lead to prosecution. The District has all rights to disable this account prior to the completion of the year if it sees fit to do so. The following guidelines will guard against someone finding out your password and using your account illegally:

1. Make your password as **long as possible**. The longer it is, the more difficult it will be to attack the password with a brute-force search. Always use at least 8 characters in your password, at least two of which are numeric.
2. **Use as many different characters as possible** when forming your password. Use numbers, punctuation characters and, when possible, mixed upper and lower-case letters. Choosing characters from the largest possible alphabet will make your password more secure.
3. **Do not use personal information** in your password that someone else is likely to be able to figure out. Obviously, things like your name, phone number, and address are to be avoided. Even names of acquaintances and the like should not be used.
4. Do not use words, geographical names, or biographical names that are **listed in standard dictionaries**.
5. Never use a password that is **the same as your username**.
6. Do not use passwords that are **easy to spot while you're typing them in**. Passwords like 12345, qwerty (i.e., all keys right next to each other), or nnnnnn should be avoided.
7. Change your password often.

Note: Approval notification with instructions will be provided via email once approved and processed

Reason for Access:

User Signature:	**Date :**
Supervisors Approval	**Date :**
Title and Signature:	

For Operator Use only

Approved_____ Denied_______	Creation Date:
Signature:	Date:

Notes:

Revised 4/16/14

Children's Internet Protection Act

Background

The Children's Internet Protection Act (CIPA) is a federal law enacted by Congress to address concerns about access to offensive content over the Internet on school and library computers. CIPA imposes certain types of requirements on any school or library that receives funding for Internet access or internal connections from the E-rate program – a program that makes certain communications technology more affordable for eligible schools and libraries. In early 2001, the FCC issued rules implementing CIPA.

What CIPA Requires

- Schools and libraries subject to CIPA may not receive the discounts offered by the E-rate program unless they certify that they have an Internet safety policy that includes technology protection measures. The protection measures must block or filter Internet access to pictures that are: (a) obscene; (b) child pornography; or (c) harmful to minors (for computers that are accessed by minors). Before adopting this Internet safety policy, schools and libraries must provide reasonable notice and hold at least one public hearing or meeting to address the proposal.
- Schools subject to CIPA are required to adopt and enforce a policy to monitor online activities of minors.
- Schools and libraries subject to CIPA are required to adopt and implement an Internet safety policy addressing: (a) access by minors to inappropriate matter on the Internet; (b) the safety and security of minors when using electronic mail, chat rooms and other forms of direct electronic communications; (c) unauthorized access, including so-called "hacking," and other unlawful activities by minors online; (d) unauthorized disclosure, use, and dissemination of personal information regarding minors; and (e) measures restricting minors' access to materials harmful to them.

Schools and libraries are required to certify that they have their safety policies and technology in place before receiving E-rate funding.

- CIPA does not affect E-rate funding for schools and libraries receiving discounts only for telecommunications, such as telephone service.
- An authorized person may disable the blocking or filtering measure during use by an adult to enable access for bona fide research or other lawful purposes.
- CIPA does not require the tracking of Internet use by minors or adults.