

UNDERSTANDING THE E-RATE PROGRAM:

ADVANCED EDITION

YEAR 17 EDITION

2014-2015 FUNDING CYCLE

Table of Contents

Program Compliance and Commitment Adjustment	3
FCC Registration Numbers	4
Competitive Bidding Process	5
Children’s Internet Protection Act	7
Leased On-Premise Equipment Eligibility	8
Resources	9
Appendix A: Sample Internet Safety Policy	
Appendix B: E-Rate Application Flow Chart	

Program Compliance and Commitment Adjustment **(COMAD)**

The E-Rate program can be confusing as described in the beginner's handbook. In many cases applicants will receive funding but failed to comply with all program rules. If such errors are discovered, the Schools and Libraries Division (SLD) is mandated by the Federal Communications Commission (FCC) to adjust the funding commitment to reflect proper payment. There are two inevitable truths regarding commitment adjustments; 1. A commitment adjustment occurs AFTER a commitment has been issued (and sometimes funds disbursed) and 2. A commitment is NEVER adjusted to increase funding.

This is the list of program rule violations that can result in a COMAD:

- Competitive Bidding Violations
- Lack of Necessary Recourses (post commitment Item 25 audit)
- Improper Service Substitution
- Failure to pay Non-Discounted Share
- Duplicate Services
- Failure to Complete Service within Funding Year
- Discount Calculation Violation
- Funded equipment moved in less than three years or missing equipment
- Services not provided for the full year
- Technology Plan not approved or does not cover entire fund year (for Priority 2 funding)
- Not CIPA compliant (no Internet Safety Policy, filtering, or public hearing)
- Waste, Fraud, or Abuse

Applicants must keep all documentation verifying compliance of all E-Rate regulations for a minimum of five years after the last date to receive service. In the event services were rendered under a multi-year contract, all documentation related to the competitive bidding process, including winning and losing bid response, bid evaluation and resulting contract. For a five year contract, the effective retention requirement would be over 10 years.

The Schools and Libraries Division has provided guidance on document retention on the SLD Web site including a link to the FCC Order: <http://usac.org/sl/tools/document-retention.aspx>

A link to a brief explanation of COMADs is here: <http://usac.org/sl/applicants/before-youre-done/commitment-adjustments.aspx>

FCC Registration Numbers

The SLD has posted revised guidance for compliance with a requirement by the Federal Communications Commission (FCC) that all schools, libraries, service providers, consultants, consortium leaders, and any entity that files a Form 470 or 471 obtain a registration number from the FCC (FCC RN). This requirement has been imposed quite simply to allow the FCC to enforce its regulations on all E-Rate participants, particularly fines and funding recovery.

Specific instructions for obtaining an FCC RN are available at:

<https://fjallfoss.fcc.gov/coresWeb/publicHome.do>

All Billed Entities and vendors must have at least ONE FCC RN.

Competitive Bidding Process

The FCC Sixth Report and Order (FCC 10-175) codified its requirement for open and fair bidding process. E-Rate gift rules are equivalent to those of federal agencies. A complete summary of federal rules for gifts and links to the set of federal regulations is available online: <http://www.oge.gov/Topics/Gifts-and-Payments/Gifts--Payments/>. The safest course of action is *not* to accept any gifts at all from participating and/or potential E-Rate suppliers. Gift prohibitions are always applicable, not just during the competitive bidding process.

When considering bids or responses from potential vendors, the price of *eligible* services must be given the highest weight. For example if two bids from cellular service providers are received and the response from one vendor will require the purchase of new phones, the cost of the replacement phones cannot be counted in the price category. Evaluation criteria may include a category for overall cost of the project but price of the eligible service must have a higher weight.

Failure to adhere to E-Rate requirements that price of eligible services must be the primary consideration when considering Form 470 responses will result in funding denial. If audited, all bids and evaluation sheets may be requested for at least five years after the last date to receive services. If required documents cannot be produced during an audit, applicants may be required to repay funds to the program (COMAD). It is advisable to keep all E-Rate required documentation in a central location for the duration of the retention period. For example, local retention policies for procurement documents may differ from E-Rate regulations and premature destruction of bid responses or evaluation sheets could result in a COMAD.

The Schools and Libraries Division provided guidance on Form 470 and competitive bidding preparation in a News Brief dated February 7, 2014:
http://www.eratecentral.com/sld_news_briefs/529.pdf

Internal Connections

E-Rate funding is split into two categories – Priority 1 (P1) and Priority 2 (P 2). Priority 1 is for information transport services such as local and long distance telephone service, cellular service, broadband telecommunications and Internet access. Priority 2 funding is provided for communication equipment within the school building, including switches, routers, cabling, and installation of eligible equipment. Generally, end user equipment such as computers, monitors and phones are not eligible for funding under P2.

Priority 2 funding is only available after all P1 services have been funded and sufficient funds are available for equipment. Because overall funding for the E-Rate program is capped, there is rarely enough funding available for all Priority 1 and 2 requests. In an attempt to provide P2 funding to more applicants, the FCC enacted regulations limiting P2 funding at individual locations to no more than two of any five given years. This is known as the two-in-five rule. Despite the rule, P2 funding demand at the highest discount levels remains very high. Consequently, applications for P2 are rarely funded below 81 percent. In fund year 2013 the

SLD board voted to recommend the FCC deny all P2 funding because of a lack of funding. When considering applications for P2 funding, applicants should consider grouping high discount schools on P2 applications.

Internal Connection Maintenance

Maintenance of internal connections is eligible for funding and is exempt from the *two-in-five year rule*. According to the Sixth Report and Order, unbundled warranties are no longer eligible. Maintenance contracts must be for a specified amount of work but may include estimates for repair of broken equipment and emergency repairs, but reimbursement will only be made for actual maintenance or repair bills. Any contract for maintenance must be limited to **ONLY** maintenance of E-Rate eligible equipment.

Children's Internet Protection Act (CIPA)

In December 2000, Congress passed the Children's Internet Protection Act (CIPA) requiring recipients of certain federal funds to protect children from pornographic, inappropriate or child pornographic Internet sites.

For E-Rate, the Federal Communications Commission established regulations for CIPA compliance. The FCC determined that applicants must develop an Internet safety policy that included a public hearing. A public hearing could include a regular board meeting with the Internet safety policy on the public agenda. **The public hearing must be documented and could result in COMAD documentation cannot be provided on request.** The policy must address the following issues:

- access by minors to inappropriate matter on the Internet and WorldWide web;
- the safety and security of minors when using electronic mail, chat rooms, and other forms of direct electronic communications;
- unauthorized access, including so-called "hacking," and other unlawful activities by minors online;
- unauthorized disclosure, use, and dissemination of personal information regarding minors; and
- measures designed to restrict minors' access to materials harmful to minors.

The regulations are clear that the level of compliance with CIPA is left entirely to local authorities. Part of the reason is a local control issue, and part is because the FCC recognizes that very few (if any) Internet filters are 100 percent effective and it would be futile to dictate which filters applicants should use. Indeed, contained within the CIPA legislation is a provision that the FCC should evaluate different filters and report on their effectiveness.

New Requirements under CIPA – Schools Only

FCC Order: FCC 11-125

http://transition.fcc.gov/Daily_Releases/Daily_Business/2011/db0819/FCC-11-125A1.pdf

- Internet safety policy must provide for the education of minors about appropriate online behavior.
- Applicants, who have existing and properly adopted Internet Safety Policies, will not be required to hold new public hearings to amend their policies, unless required by local regulations.
- Applicants must retain Internet Safety Policy documentation.
- The Order clarifies that the determination of what matter is considered inappropriate for minors is a local decision.
- The new Internet Safety Policy requirement became effective in Fund Year 2012.

The Schools and Libraries Division has provided guidance on CIPA in a News Brief dated June 14, 2013: http://www.eratecentral.com/sld_news_briefs/492.pdf

Leased On-Premise Equipment Eligibility

A bundled service that many vendors are offering is the lease of a component that resides at the school. Cable companies for example often offer to lease a router as part of their standard service. Such arrangements are eligible for funding if certain conditions are met.

The on-premise Priority 1 equipment must be an integral component of the telecommunications or Internet access service. Discounts for services that include charges for on-premise Priority 1 equipment are permissible when the following conditions are met:

- The on-premise equipment will be provided by the same service provider that provides the eligible telecommunications or Internet access service of which it is a part.
- Responsibility for maintaining the equipment rests with the service provider, not the school.
- Ownership of the equipment will not transfer to the school in the future, and the relevant contract or lease does not include an option to purchase the equipment by the school.
- Upfront, capital charges of the on-premise equipment are less than 67% of total charges (recurring plus non-recurring) in the funding year.
- The equipment will not be used by the school for any purpose other than receipt of the eligible telecommunications or Internet access service of which it is a part.
- The Local Area Network of the school is functional without dependence on the equipment.
- There is no contractual, technical, or other limitation that would prevent the service provider from using its network equipment in part for other customers. This condition often leads to confusion. Many applicants believe they have exclusive use of the equipment reasoning that it is part of the Wide Area Network and resides at the school. If the vendor can remotely connect to the device for diagnostics or repair, the school does not have exclusive use of the equipment.

Fiber

Lease of fiber, lit or dark, is eligible as a Telecom or Internet Access service from any provider, including non-profit and government agencies, and utility companies, as long as it is the most cost-effective solution. Please note; dark fiber must be lit immediately. Maintenance and installation costs of dark fiber are eligible. Construction beyond the property line and modulating equipment for leased dark fiber is *ineligible*. To be eligible requests for “fiber lease” must be posted in the P1 category on the Form 470.

Community Use of Schools’ E-Rated Services

After school hours, schools may open their facilities to the general public to use E-Rate supported services. Schools are not required to provide such access, they can decide to provide access or not. Service must primarily be for educational purposes and cost must be incidental and not increase E-Rate costs. Schools cannot charge the public to access the Internet but may charge a room fee, cleaning fee, or computer use fee.

Resources

Federal Communications Commission (FCC): <http://www.fcc.gov>

The Federal Communications Commission is the federal agency responsible for enacting regulations governing the E-Rate program.

Universal Service Administrative Company (USAC): <http://www.usac.org/sl>

USAC was created by FCC order to administer the program. The Schools and Libraries Division of USAC is responsible for administration of the federal E-Rate program.

Webinar: E-Rate for Beginners, produced by E-Rate Central in conjunction with Web Junction:

http://www.webjunction.org/events/webjunction/E-Rate_for_Beginners.html

(produced February 2011 so it is somewhat dated)

NJDOE Office of Educational Technology:

<http://www.state.nj.us/education/techno>

E-Rate Central: <http://www.E-Ratecentral.com>

E-Rate Central is an E-Rate consulting company based in New York. The Web site includes tools for schools to monitor E-Rate applications and funding. E-Rate Central is a sub-contractor for the New Jersey Digital Readiness for Learning and Assessment program.

Sandy O'Neil: NJ State E-Rate Coordinator sandy.oneil@doe.state.nj.us

NJ Department of Education

(609) 777-4662

Greg Weisiger (E-Rate Central) eratel@aol.com

(804) 302-4406

Greg works for E-Rate Central. He is available to provide assistance with implementation of the Digital Readiness for Learning and Assessment program. Greg is the current state E-Rate coordinator for Virginia libraries and former state coordinator for Virginia schools.

Sample CIPA-Compliant INTERNET SAFETY POLICY

Note: The following Internet safety policy was developed by E-Rate Central solely to address the basic policy compliance requirements of CIPA and NCIPA for E-Rate funding. Schools and libraries adopting new or revised Internet policies may wish to expand or modify the sample policy language (as suggested in the accompanying Primer) to meet broader policy objectives and local needs. Neither the FCC nor the SLD has established specific standards for a CIPA-compliant Internet safety policy and neither has reviewed, much less endorsed, this sample policy.

INTERNET SAFETY POLICY For <School or Library>

Introduction

It is the policy of <School or Library> to: (a) prevent user access over its computer network to, or transmission of, inappropriate material via Internet, electronic mail, or other forms of direct electronic communications; (b) prevent unauthorized access and other unlawful online activity; (c) prevent unauthorized online disclosure, use, or dissemination of personal identification information of minors; and (d) comply with the Children’s Internet Protection Act [Pub. L. No. 106-554 and 47 USC 254(h)].

Definitions

Key terms are as defined in the Children’s Internet Protection Act.

Access to Inappropriate Material

To the extent practical, technology protection measures (or “Internet filters”) shall be used to block or filter Internet, or other forms of electronic communications, access to inappropriate information. Specifically, as required by the Children’s Internet Protection Act, blocking shall be applied to visual depictions of material deemed obscene or child pornography, or to any material deemed harmful to minors.

Subject to staff supervision, technology protection measures may be disabled or, in the case of minors, minimized only for bona fide research or other lawful purposes.

Inappropriate Network Usage

To the extent practical, steps shall be taken to promote the safety and security of users of the <School or Library> online computer network when using electronic mail, chat rooms, instant messaging, and other forms of direct electronic communications.

Specifically, as required by the Children’s Internet Protection Act, prevention of inappropriate network usage includes: (a) unauthorized access, including so-called ‘hacking,’ and other unlawful activities; and (b) unauthorized disclosure, use, and dissemination of personal identification information regarding minors.

Education, Supervision and Monitoring

It shall be the responsibility of all members of the <School or Library> staff to educate, supervise and monitor appropriate usage of the online computer network and access to the Internet in accordance with this policy, the Children’s Internet Protection Act, the Neighborhood

Children’s Internet Protection Act, and the Protecting Children in the 21st Century Act. Procedures for the disabling or otherwise modifying any technology protection measures shall be the responsibility of <Title> or designated representatives.

[For schools only] The <Title> or designated representatives will provide age appropriate training for students who use the <School’s> Internet facilities. The training provided will be designed to promote the <School’s> commitment to:

- a. The standards and acceptable use of Internet services as set forth in the <School’s> Internet Safety Policy;
- b. Student safety with regard to:
 - i. safety on the Internet;
 - ii. appropriate behavior while on online, on social networking Web sites, and in chat rooms; and
 - iii. cyberbullying awareness and response.
- c. Compliance with the E-Rate requirements of the Children’s Internet Protection Act (“CIPA”).

Following receipt of this training, the student will acknowledge that he/she received the training, understood it, and will follow the provisions of the District's acceptable use policies.

Adoption

The Board of <School or Library> adopted this Internet Safety Policy at a public meeting, following normal public notice, on <Month, Day, Year>.

CIPA definitions of terms:

TECHNOLOGY PROTECTION MEASURE. The term “technology protection measure” means a specific technology that blocks or filters Internet access to visual depictions that are:

1. **OBSCENE**, as that term is defined in section 1460 of title 18, United States Code;
2. **CHILD PORNOGRAPHY**, as that term is defined in section 2256 of title 18, United States Code; or
3. Harmful to minors.

HARMFUL TO MINORS. The term “harmful to minors” means any picture, image, graphic image file, or other visual depiction that:

1. Taken as a whole and with respect to minors, appeals to a prurient interest in nudity, sex, or excretion;
2. Depicts, describes, or represents, in a patently offensive way with respect to what is suitable for minors, an actual or simulated sexual act or sexual contact, actual or simulated normal or perverted sexual acts, or a lewd exhibition of the genitals; and
3. Taken as a whole, lacks serious literary, artistic, political, or scientific value as to minors.

SEXUAL ACT; SEXUAL CONTACT. The terms “sexual act” and “sexual contact” have the meanings given such terms in section 2246 of title 18, United States Code.

Schools & Libraries (E-Rate) Process I FOR APPLICANTS

