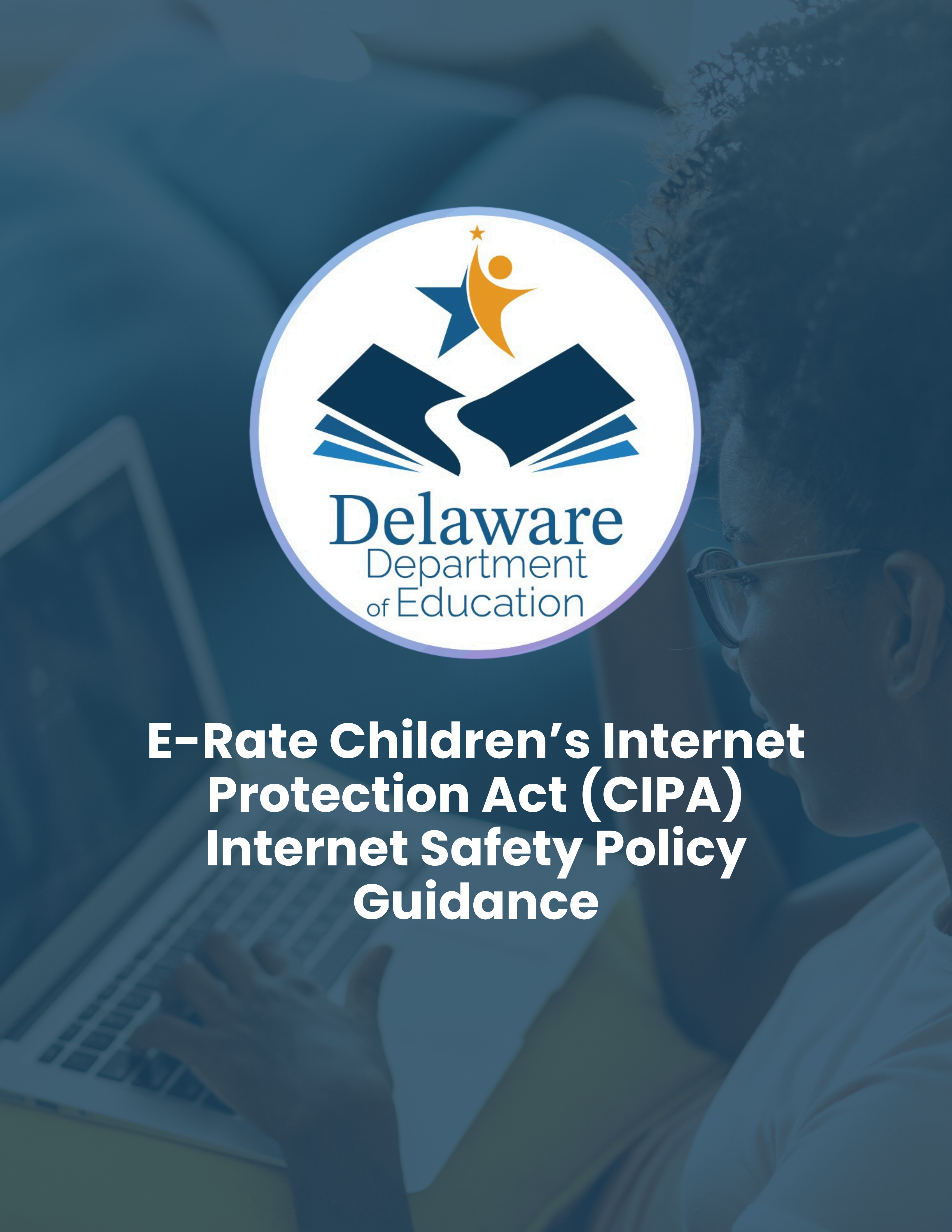

Delaware Department of Education

E-Rate Children's Internet Protection Act (CIPA) Internet Safety Policy Guidance

CIPA Internet Safety Policy Requirements (Non-Negotiable)

- **Districts and charter schools must create, approve, and distribute one or more Internet safety policies (ISP)**
    - Many districts and charter schools nationwide use their Acceptable Use Policy (AUP) as their Internet Safety Policy.

- **The school board or governing body must approve the Internet Safety Policy.**
    - Before the adoption of the ISP, the district or charter school must provide reasonable notice to the public and hold at least one public hearing or meeting.

- **Documentation of the Policy and board/governing body approval must be kept on record for 10 years for each year E-Rate funds are received. Documentation includes:**
    - Copy of the ISP(s)
    - Agenda for the public/board meeting at which the ISP will be addressed and/or adopted
    - Minutes for the public/board meeting at which the ISP will be addressed and/or adopted

- **Internet Safety Policy must address:**
    - Access by minors to inappropriate content on the Internet
    - Measures taken to restrict/filter access to inappropriate content
        - Documentation of protection measures that block or filter Internet access to content that are
            - Obscene
            - Pornographic material
            - Harmful to minors (for computers that are accessed by minors)
            - NOTE: All internet access, even use by adults, must be filtered
    - Monitoring the online activities of minors
    - Safety and security of minors when using electronic mail, chat rooms, and other forms of direct electronic communication
    - Unauthorized access, including “hacking” and other unlawful activities by minors online
    - Unauthorized disclosure, use, or dissemination of personal information regarding minors

Reference: FCC Children’s Internet Protection Act

Additional CIPA Requirements (Applicable to all districts and charter schools)

- **Children's Internet Protection Act (CIPA) Education Requirements** (FCC 11-125)**. LEAs must educate minors about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms, as well as cyberbullying awareness and response.**
    - Documentation must maintain (for 10 years per each year of funding received) a set of documents that verifies CIPA/E-Rate Compliance, including:
        - **Scope and Sequence** of the lessons being taught, including grade level, as aligned to the three federally required content areas:
            - Appropriate Online Behavior
            - Social Networking
            - Cyberbullying Awareness and Response
        - **Curriculum and/or Resource Documentation**
            - ISAFE Resources - this information is stored in ISAFE's administrative portal only if educators are logging into the system, downloading curriculum assets, and certifying
            - Other Resources – must keep detailed records of the curriculum and/or resources used
        - **Implementation Documentation**
            - Teacher names, dates, lessons taught, and the number of students, etc., that demonstrate the Internet safety curriculum and/or resources have been implemented during the school year
                - ISAFE Resources - this information is stored in ISAFE's administrative portal only if educators are logging into the system, downloading curriculum assets, and certifying
                - Other Resources
                    - Must keep detailed records of the implementation details

Documentation and Compliance Process (Applicable to all district and charter schools)

Documentation and Compliance consist of CIPA Internet Safety Instruction requirements and Internet Safety Policy compliance.

- **CIPA Education Requirements**
  - Occurs annually
  - Is documented in conjunction with Delaware Media Literacy Requirements
  - Detailed information is available in the E-Rate CIPA Internet Safety Instruction Guidance

- **Internet Safety Policy Documentation**
  - Occurs every 2 years
    - Submitted in SY 22-23
    - Review & Submit in SY 24-25
    - Review & Submit in SY 26-27
    - Review & Submit in SY 28-29
    - Etc.
  - Time-line
    - Submission process opens January 1
    - Submissions are due June 30
  - Utilize the CIPA Internet Safety Policy Evidence Collection form to submit evidence
    - Delaware E-Rate consultant, DOE, and DTI are available to provide support
  - If the district/charter school determines mid-cycle changes are necessary, additional evidence can be submitted utilizing the CIPA Internet Safety Policy Evidence Collection form

CIPA Definition of Terms

MINOR. The term “minor” means any individual who has not attained the age of 18 years.

  - Reference: COPPA 2.0: The New Battle Over Privacy, Age Verification, Online Safety & Free Speech (Page 6)

TECHNOLOGY PROTECTION MEASURE. The term “technology protection measure" is a specific technology designed to block or filter Internet access to certain types of visual depictions that are:

  - OBSCENE, as that term is defined in Section 1460 of Title 18, United States Code
  - This typically includes content that appeals to the prurient interest, depicts sexual conduct patently offensively, and lacks serious literary, artistic, political, or scientific value.
    - The legal definition of obscenity is typically drawn from the U.S. Supreme Court case Miller v. California, 413 U.S. 15 (1973). According to the "Miller Test" established in this case, material is considered obscene if:
    - The average person, applying contemporary community standards, would find that the work, taken as a whole, appeals to the prurient interest;
    - The work depicts or describes, in a patently offensive way, sexual conduct or excretory functions specifically defined by applicable state law and
    - The work, taken as a whole, lacks serious literary, artistic, political, or scientific value.
  - Reference: Citizen’s Guide to U.S. Federal Law on Obscenity

PORNOGRAPHY or CHILD PORNOGRAPHY. As those terms are defined in Section 2256 of Title 18, United States Code

  - Generally, pornography refers to explicit representations of sexual conduct, while child pornography specifically involves such representation involving a minor
  - Reference: U.S.C. Title 18, Chapter 110

HARMFUL TO MINORS, as those terms are defined in compliance with the Children’s Internet Protection Act (CIPA)

  - “harmful to minors” is defined as any picture, image, graphic image file, or other visual depiction that:
    - Taken as a whole and concerning minors, it appeals to a prurient interest in nudity, sex, or excretion

    - 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.
    - Taken as a whole, lacks serious literary, artistic, political, or scientific value as to minors.
  - Reference: Universal Service Administrative Co. (USAC) CIPA

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.

  - Generally, contact involves sensitive body parts or areas, and in the case of this description, contact includes interaction between the mouth and/or sensitive body parts or areas. In addition, the term "personal interaction" signifies the purposeful touching, whether directly or through clothing, of private body parts, with the intention of causing harm, embarrassment, distress, degradation, or to create sexual excitement.
  - Reference: United States Code, Title 18, Section 2246

ACCESS TO INAPPROPRIATE MATERIAL. The term "access to inappropriate material" refers to the ability to reach and view content on the internet that is obscene, pornographic, or harmful to minors as defined by Section 1460 and 2256 of Title 18, United States Code.

  - Reference: Citizen’s Guide to U.S. Federal Law on Child Pornography

SAFETY AND SECURITY WHEN USING ELECTRONIC MAIL, CHAT ROOMS, AND OTHER FORMS OF DIRECT ELECTRONIC COMMUNICATIONS. This term relates to the provision of protection measures that prevent harm, threats, or violations of privacy when minors engage in direct digital communications, such as emails and chat rooms.

UNAUTHORIZED ACCESS, INCLUDING SO-CALLED “HACKING,” AND OTHER UNLAWFUL ACTIVITIES BY MINORS ONLINE. This phrase refers to the illegal actions by minors to bypass security protocols, gain unauthorized access to systems or data (commonly known as "hacking"), or carry out other unlawful online activities.

UNAUTHORIZED DISCLOSURE, USE, AND DISSEMINATION OF PERSONAL IDENTIFICATION INFORMATION REGARDING MINORS. This term indicates any unauthorized act of revealing, employing, or spreading personal identification data about minors in violation of privacy and data protection regulations.

RESTRICTION OF MINOR'S ACCESS TO MATERIALS HARMFUL TO THEM. This term refers to the enforcement of technology measures or strategies that limit a minor's ability to access online content that is deemed harmful to their well-being or development.

SUPERVISING ADULT. The term "supervising adult" refers to an adult who is responsible for monitoring and guiding a minor's use of internet access within a school or library setting.

ONLINE BEHAVIOR. The term "online behavior" relates to the actions, interactions, and practices of individuals when using the internet, including social networks, email communications, online gaming, and web browsing.

EDUCATIONAL INSTITUTION. The term "educational institution" includes schools, libraries, and any other establishments that offer formal education to minors and have access to the Internet.

INTERNET SAFETY POLICY. The term "Internet safety policy" refers to a set of rules or guidelines formulated to promote safe and appropriate use of the internet within a school, library, or other educational institutions. This includes strategies for the protection of minors from harmful online content and for ensuring their privacy and security in online activities.

PUBLIC OR PRIVATE FUNDING. The term "public or private funding" refers to financial resources provided by either governmental entities or private organizations, utilized for educational purposes, including internet access and technology protection measures in schools and libraries.

These definitions are derived from the Children’s Internet Protection Act CIPA and are intended to provide clarity and consistency in its interpretation and implementation. They are not exhaustive and may need to be supplemented or updated based on changes in law, technology, or societal norms.

Resource: FCC Children’s Internet Protection Act (CIPA)
Resource: Federal Trade Commission Children’s Privacy

Internet Safety Policy (ISP) Elements to Consider

The “ISP Elements to Consider” included in this guidance are solely intended to assist Delaware districts and charter schools as they create, review, and/or update their Internet Safety Policies. Decisions are discretionary at the district and charter school level. This document is intended to provide suggested best practices.

Processes

- **Formalized Communication Process, Including Suggested Stakeholders**
  - District/Charter stakeholders
    - Internet Safety Policy
      - Technology Managers/Information Security Officer
      - Instructional Technology Specialists
      - Business Managers
      - District Office Staff
      - Superintendent/Charter Lead
      - Public Communications Officer
      - Equity Officer/Specialist
  - CIPA Education Requirements/Media Literacy Requirements
    - Instructional Technology Specialists
    - Curriculum Directors
    - District Office Staff
    - Superintendent/Charter Lead
    - Equity Officer/Specialist
- **Student Involvement**
  - Include students in ISP development/review/revision processes
  - Include students in open dialog regarding the ISP(s) to support student understanding
    - Resource: US DOE Office of Educational Technology Student-Centered Acceptable Use Policy
- **Process for Evaluating/Reviewing New Technologies and Tools**
  - Description of district/charter process
  - Elements that are involved in evaluation processes
  - Resources that can be used in evaluation process
  - Evaluation criteria
- **Consider Alignment of ISP/AUP to Student Handbook/Code of Conduct**
  - Elements to consider including in ISPs (not an exhaustive list)
    - Electronic communications staff/students
    - Social networking
    - Cyberbullying
    - Intellectual property

        - Safe and Ethical use of AI
        - Cyberdating/sextortion
        - Drugs and alcohol online
        - Maintenance and care of equipment
        - Personal responsibility
        - Notice of intent to monitor
        - Gambling
        - Multi-factor Authentication (MFA)
        - Electronic communication
            - Staff to staff
            - Staff to students
            - Students to students
- **ISPs/AUPs Differentiated by Grade Band**
    - Format
        - Separate documents
        - One document with grade band elements differentiated
        - One document including common elements, then differentiating by grade band where necessary
    - Comprehensive ISP/AUP with family/student-friendly information/clarifications included
    - Process for including students in the development/review of the ISP/AUP
    - Example of Student AUP
        - Example: Houston Independent School District AUP
        - Example: Houston Independent School District Condensed AUP
- **Specifications for Staff Members with Elevated Rights**
    - Collaborate with Human Resources
- **Accessibility**
    - ISP/AUP available in multiple languages
    - ISP/AUP document created in compliance with WCAG 2.1, Level AA
    - ISP/AUP available in alternate accessible formats
- **Authorized Use of Technology and Accounts**
    - Process/policy for utilizing authorized login only
    - Process/policy for shared and/or spare devices
        - Address logging user access
        - Address managing inventory
    - Process for Substitute accounts
- **Reference CIPA & Best Practice Web Filtering Consideration for LEA's document (DOE & DTI)**
    - Contact district/charter, TechMaCC, or Digital Learning Cadre (DLC) representative. The document is shared with TechMaCC and DLC and can be found in the Edu Technology Resources Team - TechMaCC channel - Content Filtering folder.

Other Elements to Consider

Training/Professional Development

- How will your district/charter school provide Internet Safety Policy/AUP training for staff and students
    - How will you address training for staff
        - Modality
        - Timing
        - Frequency
        - Accountability
    - How will you address training for students
        - Modality
        - Timing
        - Frequency
        - Accountability

Legal Notice

This resource may contain links to websites operated by third parties. These links are provided for your convenience only and do not constitute or imply any endorsement or monitoring by DDOE.