NATIONAL CHARTER SCHOOLS INSTITUTE

Administrative Guidelines

REVISED GUIDELINE – SPRING 2023 –
WEB-CONTENT AND FUNCTIONALITY SPECIFICATIONS

DRAFTING NOTE: ***"Responsive" design "uses CSS (Cascading Style Sheets) technology to create a single version of a website that auto-adjusts to display properly on all devices except the oldest cellphones." "Adaptive" design "detects and identifies the user's device and then generates a page matched to the device capabilities." ("How to Make Your Website More Mobile-Friendly" – https://www.entrepreneur.com/article/226575 [accessed 7/7/2016])***

This guideline and AG 5723 and AG 7540 and Form 7540.03 F1, Form 7540.04 F1, and Form 7540 F4 ~~will~~ apply to all web content hosted on the Board's servers or Academy-affiliated servers, or provided through the Academy's website(s)/web pages, whether created by staff, students, or contracted third parties. The **[ ] School Leader [ ] Educational Service Provider** ~~School Leader (employed by the Board)~~ retains final editorial authority over all content ~~placed~~ hosted on the Board's servers or Academy-affiliated servers and displayed on the Board's website(s). The **[ ] School Leader [ ] Educational Service Provider** retains the authority to remove content or links from any web page the **[ ] School Leader [ ] Educational Service Provider** determines is inappropriate. ~~(employed by the Board) has the right to remove pages or links from any web page based upon his/her determination of inappropriate content.~~

The Academy's Web Accessibility Coordinator is charged with implementing these guidelines. The Web Accessibility Coordinator can be reached at:

[Insert address/phone number/e-mail address]

_____

_____

_____

The Academy's website(s) serve(s) as instructional, communication, and public relations tools. The content on the website(s) aims ~~web pages aim~~ to provide timely, supportive, and educational information to students, parents, staff, and the community. The website(s) are created in order to facilitate access to a wide variety of rich media and educational resources that directly support student achievement, professional development, and organizational effectiveness.

[ ] The Academy strives to deliver a website(s) that ~~is/are ( ) responsive ( ) adaptive so it/they~~ can be viewed in an optimal manner **( )** on a computer and mobile device **( )** all devices. **[END OF OPTION]** **( )** To maximize accessibility and usability, it is recommended that web content be presented in a simple page design, employ large font sizes and big, touchable buttons that accommodate larger fingers, and place critical information "above the fold." Further, the individuals responsible for the web design and content shall take into consideration and utilize the following practices:

A. **Color contrast in text.** Use sufficient color contrast between the text and the background so individuals with limited vision or color blindness can read text that uses color.

B. **Text cues when using color in text.** When using text color to provide information (such as red text to indicate required form fields), include text cues for individuals who cannot perceive the color. For example, include the word "Required" in addition to red text for required form fields.

C. **Text alternatives ("alt text") in images.** Employ text alternatives to convey the purpose of an image, including pictures, illustrations, charts, etc., so individuals who do not see the image, such as people who are blind, can use screen readers to hear the alt text read out loud. Such text should be short and descriptive.

D. **Video captions.** Include synchronized captions that are accurate and identify any speakers in the video.

E. **Online forms.** When developing forms, be sure to include labels, clear instructions, and keyboard access. The labels will allow individuals who are blind and use screen readers to understand what to do with each form field (e.g., explaining what information goes in each box of a job application form). Additionally, design the form so that individuals who use screen readers are automatically informed when they enter a form field incorrectly. The notice should clearly identify the error and how to resolve it (e.g., an automatic alert tells the user that a date was entered in the wrong format).

F. **Text size and zoom capability.** Make sure the web design allows for individuals with vision disabilities to use a browser's zoom capabilities to increase the size of the font so they can see things more clearly.

G. **Headings.** When sections of a website are separated by visual headings, build the headings into the website's layout so that individuals who are blind can use them to navigate and understand the layout of the page.

H. **Keyboard and mouse navigation.** Design the website/web page(s) so as to allow for keyboard access (i.e., so users can navigate web content using keystrokes, rather than a mouse).

I. **Checking for accessibility.** While it is appropriate and beneficial to use automated accessibility checkers and overlays to identify or fix problems with the website/web page, pair the use of such automated checkers with a manual check of the website/web page to verify its accessibility.

J. **Reporting accessibility issues.** Include on the website(s) a way for the public to report accessibility problems so the Academy can fix any accessibility issues.

Additionally, key information such as the Academy's name, contact information, and a link to a table of content/site map should be placed in the top left corner of the home page so it is easy to find.

[END OF OPTION]

Website Accessibility

The Academy's website(s) operate(s) in compliance with Federal and State law. As such, the Academy is committed to providing individuals with disabilities with an opportunity equal to that of their nondisabled peers to participate in the Academy's programs, benefits, and services, including those delivered through electronic and information technology. To this end, the Technology Director is charged with verifying the Academy's website(s) allow(s) persons with disabilities to acquire the same information, engage in the same interactions, and enjoy the same benefits and services within the same timeframe as their nondisabled peers, with substantially equivalent ease of use, not be excluded from participation in, denied the benefits of, or otherwise be subjected to discrimination in any Academy programs, services, and activities delivered online, as required by Federal and State law, and receive effective communication with Academy programs, services, and activities delivered online.

[ ] The Academy measures the accessibility of online content and functionality according to the World Wide Web Consortiums (W3C's) Web Content Accessibility Guidelines (WCAG) 2.0 and the Web Accessibility Initiative Accessible Rich Internet Applications Suite (WAI-ARIA) 1.1~~1.0~~ for web content (Benchmarks for Measuring Accessibility) **( )**, which are incorporated by reference. **[END OF OPTION]. [END OF OPTIONAL SENTENCE]**

[DRAFTING NOTE: While OCR currently (as of December 2022) recommends WCAG 2.0 Level AA, WCAG 2.1 is gradually becoming the standard courts cite as the ADA accessibility standard that public entities should use for websites, mobile applications, and digital content compliance. Further, W3C published a working draft of WCAG 2.2 in August 2020 and a Candidate Recommendation draft of WCAG 2.2 in September 2022; a final version of WCAG 2.2 is expected to be released in early 2023. The W3C states that WCAG 2.0 and 2.1 remain its recommendation, but version 2.2 should be used to maximize future applicability of accessibility efforts. The W3C also encourages the use of the most current version of WCAG when developing or updating Web accessibility policies. The standards can be located at https://www.w3.org/TR/WCAG20/ and https://www.w3.org/TR/wai-aria/ (accessed 11/22/2022)]

~~***DRAFTING NOTE: OCR recommends WCAG 2.0 Level AA. The standards can be located at https://www.w3.org/TR/WCAG20/ and https://www.w3.org/TR/wai-aria/ (accessed 7/7/2016)***~~

All ~~new, newly-added and modified~~ web content and functionality must be accessible to individuals with disabilities **( )** as measured by conformance to the Benchmarks for Measuring Accessibility **[End of Option]**, except where doing so would impose a fundamental alteration or undue burden. This provision also applies to the Academy's online content and functionality developed by, maintained by, or offered through a third party~~third-party~~ vendor or through the use of open sources~~.~~ when the content pertains to the Academy's programs, benefits, and/or services. The Web Accessibility Coordinator will vet online/digital content available on the Academy's website(s)/web pages that is related to the Academy's programs, benefits, and/or services to verify compliance with the requirements of this paragraph.

Nothing in the preceding paragraph, however, shall prevent the Academy from including links on the Academy's website(s)/web pages to recognized news/media outlets (e.g., local newspapers' websites, local television stations' websites) or website(s)/web pages that are

developed and hosted by outside vendors or organizations that are not part of the Academy's program, benefits, and/or services.

When the fundamental alteration or undue burden defense applies, the Academy will provide an equally effective alternative means of accessing the web content. ~~alternate access.~~ In providing an equally effective alternative means of accessing the web content~~alternate access~~, the Academy will take any actions that do not result in a fundamental alteration or undue financial and administrative burden, but nevertheless provide that, to the maximum extent possible, individuals with disabilities receive the same benefits or services as their nondisabled peers. That said, alternatives are not required to produce the identical result or level of achievement for persons with disabilities and persons ~~and~~ without disabilities, but must afford persons with disabilities an equal opportunity to obtain the same result, to gain the same benefit, or to reach the same level of achievement, in the most integrated setting appropriate to the person's need.

[ ] Only the **[ ] School Leader [ ] Educational Service Provider,** ~~School Leader (employed by the Board),~~ after considering all resources available for use in the funding and operation of the service, program, or activity, may determine an undue burden or fundamental alternation defense is applicable. In making such a determination, the **[ ] School Leader [ ] Educational Service Provider** ~~School Leader (employed by the Board)~~ will document the reasons for ~~s/he reached~~ that conclusion **( )**, including the costs of meeting the applicable Benchmarks for Measuring Accessibility on a given website/webpage ~~web page or site~~, and the available funding and other resources **[END OF OPTION]**. Additionally, the **[ ] School Leader [ ] Educational Service Provider**~~School Leader (employed by the Board)~~ will describe how the Academy will provide an equally effective alternative means of accessing the web content. **[END OF OPTIONS]** ~~equally effective alternate access.~~

Students, employees, guests, and visitors can report violations of the technical standards or any accessibility concerns to the Web Accessibility Coordinator. The Academy's website will include on its home page and throughout the website (including all subordinate pages and sites), a Notice to persons with disabilities regarding how to request the webmaster or other appropriate person to provide access to (or notify the Academy regarding) content or functionality that is currently inaccessible. The Notice will also include information or an accessible link to information instructing individuals with disabilities how to file more formal complaints under Section 504 and/or the ADA.

~~The Academy's website will include on its home page and throughout the website (including all subordinate pages and sites), a Notice to persons with disabilities regarding how to request the webmaster or other appropriate person to provide access to (or notify the Academy regarding) content or functionality that is currently inaccessible. The Notice will also include information or an accessible link to information instructing individuals with disabilities how to file more formal complaints under Section 504 and/or the ADA. If a person has a concern with respect to a web page's accessibility, they should contact the Academy's 504 Compliance Officer(s)/ADA Coordinator(s) as identified in Policy 2260.01 – Section 504/ADA Prohibition Against Discrimination Based on Disability, or the Academy's Technology Director.~~

[ ] The Web Accessibility Coordinator will establish a system to routinely audit/test the accessibility of the Academy's online/digital content and measure it against the technical standards adopted above. This audit will occur **( )** at least annually **( )** no

less than once every two (2) years **[END OF OPTION]**. ~~The Technology Director will set up a system to routinely audit/test the accessibility of all web content and functionality.~~ This system must include processes to verify claims of accessibility by third party ~~third-party~~ vendors or open sources. The purpose of the audit is to identify any web content or functionality that is inaccessible to persons with disabilities. The person/entity who conducts the audit shall report to the School Leader ~~(employed by the Board)~~ **( )** and Technology Director **[END OF OPTION]** the results of the audit so that appropriate action can be taken to address any inaccessibility. **( )** The audit shall include the Academy's home page, all subordinate pages, and ~~School~~ Academy intranet pages and sites. **( )** The person/entity conducting the audit **( )** will **( )** may seek input from members of the public with disabilities, including parents, students, employees, and others associated with the Academy, and other persons knowledgeable about website accessibility, regarding the accessibility of the Academy's web content and functionality. **[END OF OPTION]**

The Academy will provide **( )** annually **[End of Option]** website accessibility training to all appropriate personnel~~,~~ including, but not limited to: content developers, webmasters, procurement officials, and all others responsible for developing, loading, maintaining, or auditing web content and functionality. The training will include information concerning this guideline and the employees' respective roles and responsibilities associated with verifying that web design, documents, and multimedia content are accessible. The training will be facilitated by individuals with sufficient knowledge, skill, and experience to understand and employ the technical standards identified above. **( )** The Academy will maintain documentation of the training it delivers, including a list of attendees and their positions, a description of the delivered training content, **( )** copies of the training materials, **[END OF OPTION]** and the presenter's/trainer's credentials for providing such training. **[END OF OPTIONAL SENTENCE]**

Individuals responsible for designing, developing, and producing web content are expected to employ universal design principles to create web pages and sites that allow persons with ~~the~~ disabilities **( )** identified at the end of this document **[END OF OPTION]** to access the information and content on the Academy's website. By following the web content design criteria set forth below, the designers and authors of the Academy's website(s) can improve the opportunities for persons with disabilities to access the information and content contained on the web pages that make up the Academy's website(s).

First Page of the Site

The first page of an individual academy's ~~the~~ web~~-~~site should contain:

A. the index or table of contents for the site;

B. contact information, including the ~~school's~~ academy's name, address, and phone number, the name of the building principal, and a map/directions to the building;

C. the webmaster and e-mail address of the person responsible for the site;

D. a date when the page was last updated or modified;

E. index.html;

F. a link to the Board's web site;

G. identification of (or a link to) the Board's agent to receive notification of claimed copyright infringement (including name, mailing address, telephone number, fax number, and e-mail ~~e-mail~~ address);

H. links to appropriate disclaimers.

Organization of Site Structure

A. The overall plan or file structure should provide quick access to information and help the user understand how the information is organized. It is recommended that a storyboard be used to plan the web site.

B. Each page should be designed with the audience and goal in mind.

C. A basic page format should be used, e.g., use the same background, locate navigation tools in the same place on the page, have consistent link appearance, and have consistent font size and type. Be consistent on all pages.

D. The title bar should include the ~~school~~ academy name in the <title> tag of each HTML document.

E. Limit page length, keep the HTML documents as small as possible.

( ) The web site may include areas such as staff information, student projects, calendar, ~~school~~ academy information and mission statement, technology plan, and geographical information. **[END OF OPTION]**

G. There should be a "mail to" link that provides a means of feedback on all main pages.

Keep Your Web Site Current

A. Pages should be checked regularly to ensure that links are working and meet Board standards. Check to make sure all internal and external links work properly.

B. Remove expired date-related items.

C. Maintain and update content by removing unneeded or outdated files.

Grammar and Spelling

A. All pages should be grammatically correct.

B. All words should be spelled correctly - web pages should be spell checked.

Navigation Tools

Position navigational aids throughout documents and document groups. All pages should include a "back to" main menu in order to provide a link back to the web-site index or home page, or a "skip to main content" link in the upper left corner that allows users to jump past repetitive navigation options.

( ) Backgrounds

A. Keep backgrounds simple. Light colors are better. Select backgrounds that make text easy to read.

B. Keep background tiles small.

C. Backgrounds should be in GIF format.

D. Re-use background images, pages will reload quicker and the user will be able to view your pages with ease.

E. Do not use a background to convey information.

F. Do not "name" your colors. For example, Netscape allows you to use the following tag; <body bgcolor - "green"> and your background will be green. This is a tag specific to Netscape and not necessarily supported by other browsers. Use the hexadecimal number for colored backgrounds. If using a tiled image, make the background color approximately the color of the tiled image.

G. Avoid low-contrast color combinations or colors that may not be recognized by lower-resolution screens.

[END OF OPTION]

DRAFTING NOTE: This topic is addressed in the Benchmarks for Measuring Accessibility.

Intellectual Property

A. All web-site authors must follow all applicable and existing copyright laws pertaining to the use of text, images, sounds, and hyperlinks to other web sites/web pages. (see AG 2531)

B. The Board retains proprietary rights to web-sites/web pages hosted on its servers, absent written authorization to the contrary.

Naming Structure

A. Use all lower-case letters for names of documents and graphics.

B. Do NOT use any spaces or other symbols in naming HTML documents or graphics.

Graphics/Video/Audio

A. Smaller is better, images should be less than 50k.

B. Pictures need to be in GIF or JPEG format.

C. Always use width and height tags.

D. Provide short, simple, and meaningful alternative text for all graphical features. Use the "alt" tag to describe your picture for text-only browsers.

E. Use GIF format for drawings and line art.

F. Use JPEG format for photographic color images.

G. Re-use graphics when appropriate. When graphics are re-used, they remain in the computer and will load more quickly onto a web page.

H. Avoid using flashing content, as it may cause seizures in susceptible users.

I. Provide transcripts, descriptions, or captions for video and audio files to assist persons with visual and hearing disabilities.

HTML Standards

It is reasonable to expect that users will see your page using a variety of browsers including Google Chrome, Netscape, Microsoft Internet Explorer/Edge, Apple Safari, and Mozilla Firefox. It is recommended that you:

A. test web pages on a variety of browsers, including text-only browsers and a variety of screen resolutions to confirm the pages look right to the greatest number of users;

B. check your website~~web site~~ on multiple platforms~~,~~ and test pages on small screens to confirm the pages do not bleed off the screen;

C. use standard universal recognized HTML tags - Do Not use tags that ~~which~~ are specific to one (1) browser;

D. use HTML syntax checkers to search your site for programming mistakes.

Frames and Special Formats

Do not use frame pages. If you do and you link to external content, make sure you are not infringing on any copyrights associated with the website/web page to which you are linking. Additionally, if you use frames, make alternative versions of those pages that persons with disabilities can use. To make them accessible to screen reader devices, add meaningful titles to each frame so the user can navigate between them easily.

Provide text-based delivery alternatives for as much information as possible. Do not rely solely on special formats (e.g. Adobe Acrobat) that can be more difficult for text and voice systems to read.

Use of Student Names, Pictures, Original Work, and E-Mail~~E-mail~~ Addresses

The Board permits the use of photographs of students, names of students, and displaying original work of students on web sites in accordance with the following guidelines:

( ) Identifiable photographs of students and/or student's first names may be placed on the Internet only after the appropriate release form has been signed by the student (if eighteen (18) years of age or older) or the student's parents or guardians (if the student is seventeen (17) years of age or younger). ~~parents or guardians.~~ **[NOTE: The FBI recommends that schools not post: children's names or photos; personal information about students; activity schedules. If a school publishes student pictures on the Internet, the FBI recommends only posting distant group pictures, angled heads, and faces should be unidentifiable.]**

( ) Last names of students and students' e-mail addresses should never be used.

( ) Original work by a student~~Original work by students~~ such as artwork~~art work~~, poetry, essays, performances, etc. may be placed on the web site only after the appropriate release form has been signed by the student (if eighteen (18) years of age or older) or the student's parents or guardians (if the student is seventeen (17) years of age or younger). ~~parents or guardians.~~

Prohibited Uses

Under no circumstances may a web page hosted on the Board's servers or an Academy-affiliated server be used for commercial purposes, political lobbying, or to provide financial gains for any individual. Included in this prohibition is the fact no web pages contained on the Academy's website may:

A. include statements or other items that support or oppose a candidate for public office; the investigation, prosecution, or recall of a public official; or passage of a tax levy or bond issue;

B. link to a website of another organization if the other website includes statements or other items referenced in A. above;

C. communicate information that supports or opposes any labor organization or any action by, on behalf of, or against any labor organization;

D. include defamatory, libelous, obscene, profane, vulgar, or sexually explicit matter or harassing or abusive language;~~or obscene matter;~~

E. promote alcoholic beverages, cigarettes, or other tobacco products, or any illegal product, service, or activity;

F. promote illegal discrimination on the basis of race, sex, color, religion, national origin, disability, age, or ancestry;.

G. be utilized to intimidate or bully another person.

~~Additionally, no web pages may contain obscene, profane, vulgar, sexually explicit, defamatory, harassing or abusive language, or be utilized to intimidate or bully another person.~~

Content for the Academy's Website(s)

All subject matter on web pages must relate to curriculum, instruction, academy-authorized~~school authorized~~ activities, general information, supporting student safety, growth, and learning, or public information of interest to community members. The following information/content will/may be addressed in the Academy's website(s):

NOTE: THERE ARE SIGNIFICANT ISSUES, BOTH FROM A LEGAL LIABILITY AND REASONABLE, COMMON SENSE STANDPOINT THAT NEED TO BE ADDRESSED WHEN SELECTING THE TYPE OF CONTENT TO INCLUDE ON A WEBSITE. ACADEMYS ARE ENCOURAGED TO DISCUSS THESE ISSUES WITH THEIR LEGAL COUNSEL BEFORE DECIDING ON WHAT INFORMATION TO PLACE ON WEB PAGES HOSTED BY THE ACADEMY

( ) ~~School~~ Academy Contact Information

( ) Name

( ) Physical address

( ) E-mail

( ) Web address

( ) ~~School~~ Academy Background

( ) History

( ) Mission

( ) Song

( ) Logo

( ) Virtual ~~School~~ Academy Tour

( ) Directions

( ) **Map**

( ) **Photos**

( ) **Classrooms**

( ) **Video**

( ) **Live cams**

( ) ~~School~~ Academy **Accomplishments**

( ) **Awards**

( ) **Achievement**

( ) **Grants**

( ) **Special thanks**

( ) ~~School~~ Academy **Announcements**

( ) **Events**

( ) **Schedules – including bus schedules**

( ) **Calendars**

( ) **Timeliness**

( ) **Lunch menus**

( ) **News and Information**

( ) **Agendas and minutes**

( ) **Newspaper**

( ) **Ezines**

( ) **Announcements – closings (e.g., ~~snow~~ calamity days) or delayed starts**

( ) **Employment opportunities**

( ) ~~School~~ Academy **Policies and Procedures**

( ) **Mission**

( ) **Philosophy**

( ) Handbooks

( ) Curriculum guides

( ) Policies

( ) Programs

( ) Administrative Guidelines/Regulations/Procedures

( ) People Information

( ) Staff/Administration

( ) Principal welcome

( ) Directory (name, position, contact info)

( ) Teacher pages

( ) Directory (name, position, contact info)

( ) Class or Grade Level Pages

( ) Classroom

( ) Projects

( ) Assignments

( ) Themes

( ) Field trips

( ) Student Pages

( ) Project posting

( ) Sharing

( ) Links to personal pages (off site)

( ) Support Departments

( ) Content area departments

( ) Library/Media

( ) Technology

( ) Health Services

- ( ) **Transportation, including bus routes**
- ( ) **Art and Music**
- ( ) **Sports/Athletics**
- ( ) **Clubs/Extracurricular Organizations**
- ( ) **After school programs**
- ( ) **Special programs (special education, gifted education, etc.)**

( ) **Curriculum Connections**

- ( ) **Student resources**
  - ( ) **Assignments**
  - ( ) **Course information**
  - ( ) **Projects**
  - ( ) **Popular/relevant links (developmentally appropriate, curriculum relevant content)**
- ( ) **Teacher resources**
  - ( ) **Lesson plans**
  - ( ) **Professional development**
  - ( ) **Popular/relevant links**
- ( ) **Parent resources**
  - ( ) **Parenting resources**
  - ( ) **Popular/relevant links**
- ( ) **Curriculum Materials**
  - ( ) **Online curriculum materials – lessons, activities, homework**
- ( ) **Grades**

( ) **Community Information and Outreach**

- ( ) **Local Information**

( ) Weather

( ) Geography

( ) Demographics

( ) Culture

( ) Events

( ) Attractions

( ) Library

( ) Local Resources

( ) Natural and historical resources

( ) Business and Nonprofit contacts

( ) Business Connections

( ) ~~School~~ Academy supporters

( ) Grants

( ) Free advertising

( ) Call for Participation

( ) Volunteers

( ) Wish list

( ) Funding needs

( ) Gather information/feedback from parents and community

Neither staff nor students may publish on the Academy's website personal pages or pages for individuals or organizations not directly affiliated with the Academy.

Website/Web Page Evaluation

Before ~~releasing or~~ publishing a website/web page, _____ (building principal, sponsoring teacher, central officer administrator, technology coordinator, etc.) shall evaluate ~~conduct a website/page evaluation to assess~~ the following criteria: age appropriateness (appealing and readable); content (relevant, accurate, complete, objective, current, clear and concise, informative, appropriate, links working); intellectual property issues (sources cited; sponsoring organization identified [i.e. class, school, activity]; releases obtained); and format

(accessible, navigation, searchable, functional/useable, download speed, pages dated as to creation/updated).

[ ] The Web Accessibility Coordinator will also assess the website's/web page's accessibility. ~~The Technology Director will also assess the web pages/site's accessibility.~~

Disclaimers

[ ] Links:

Links to the following disclaimers shall be utilized as appropriate on the Academy's web pages:

[CHOOSE OPTION #1, OPTION #2 OR OPTION #3]

[ ] OPTION #1

"The _____ Academy makes every effort to verify that all links are operational and all information is accurate, appropriate, and of high quality. The Academy expects that these standards are met. The viability of links that are not created through our Academy cannot be guaranteed."

[END OF OPTION #1]

[ ] OPTION #2

"Links to external websites are included if they add information that may aid the user, and are included only as a public service. Every effort is made to verify that the links are educational in nature, and related to the Academy's educational mission, but the Internet is dynamic and volatile, and web pages can change suddenly and rapidly. It is not unusual to find information or images that are objectionable. Inclusion of a link does not constitute an endorsement by the Academy of that site, or of any third party ~~third-party~~ sites to which it may be linked. The user is advised that once you leave the Academy's website(s), even through links included on these pages, you may encounter inappropriate, illegal, or inaccurate material. The Academy is not responsible for the external content or for any fees associated with the use of an outside site. Proceed at your own risk."

[END OF OPTION #2]

[ ] OPTION #3]

"The links in this area will let you leave the Academy's website(s). The linked sites are not under the control of the Academy and the Academy is not responsible for the contents of any linked sites, or any links contained in a linked site, or any changes or updates to such sites. The Academy is providing these links to you only as a convenience and the inclusion of any link does not imply endorsement of the site by the Academy."

[END OF OPTION #3]

[ ] Student-Developed ~~Student Developed~~ Web Pages: "All web pages created by students and student organizations on the Academy's website(s)/intranet computer system will be subject to treatment as academy-sponsored~~School-sponsored~~ publications. As such, the Academy reserves the right to exercise editorial control over such publications in accordance with Policy 5722 – ~~School~~Academy-Sponsored Publications and Productions."**[END OF OPTION]**

Domain Name and Copyright: "The Academy has registered its domain name(s) for the purpose of exclusive Internet identification. The Academy asserts copyright, trademark, and/or other intellectual property rights in its domain name, Academy identification, Academy logo, and all content on the Academy's website(s). All rights are reserved. Outside parties, including parents, patrons, or outside organizations may not use Academy and/or ~~school~~ academy domain names in connection with the publication of web content. Under no circumstances shall any party use Academy and/or ~~school~~ academy domain names to promote political issues, causes, or candidates."

General Disclaimer: "Information provided on the website carries no express or implied warranties as to accuracy, timeliness, or appropriateness for a particular purpose; in addition, the Board disclaims owner responsibility for content errors, omissions, or infringing material, and disclaims owner liability for damages associated with user reliance on information provided at the site."

Events: "Visitors rely on information on the website at their own risk. Times and dates are subject to change and spectators or audiences are strongly encouraged to contact the ~~school~~ academy for the most recent schedule."

[ ] [OPTIONAL LANGUAGE]

~~[ ]~~ Examples of Disabilities and How they Affect People's Abilities to Perceive and Use Websites/Pages~~.~~

Visual Disabilities:

Blindness – People with no sight typically browse the Internet using voice output software or refreshable Braille hardware. Such devices "read" what is on the screen to the user.

Low vision – Individuals who have limited vision may use screen-enlarging software.

Color blindness – To perceive color differences on a computer monitor, individuals with color blindness need high contrast. Also, designers/developers/authors should be mindful of the forms of color blindness when choosing color schemes. Typical color blindness involves the inability to distinguish between red and green, blue and green, or blue and yellow; some people see black and white only.

Auditory Disabilities:

Deafness – People who cannot hear, experience a website/web page only through its text, graphics/images, and video.

Hard of hearing – Individuals with limited hearing may use sound-enhancing peripherals.

Physical/Motor Disabilities:

People with physical disabilities or limited fine motor skills may have difficulty with the following computer-related tasks:

Detailed manipulation of input devices such as a mouse or roller ball.

Holding down multiple keyboard keys simultaneously.

Cognitive/Language Disabilities:

Typical problems for people who have cognitive disabilities or disabilities that affect their language skills include the following:

Difficulty with spatial reasoning and/or visualization skills.

Difficulty reading and/or understanding written text (e.g. persons with dyslexia).

Persons wanting to learn more about web accessibility standards and guidelines should consult the following Internet sources:

The Access Board (www.access-board.gov) - Federal agency dedicated to accessible design.

World Wide Web Consortium (www.w3.org) – organization developed "Web Content Accessibility Guidelines (WCAG) 2.0" and the “Web Accessibility Initiative Accessible Rich Internet Applications Suite (WAI-ARIA) 1.1~~1.0~~.”

[END OF OPTIONAL LANGUAGE]

REVISED GUIDELINE – SPRING 2023
STUDENT TECHNOLOGY ACCEPTABLE USE AND SAFETY

Source: P.L. 106-554, Children's Internet Protection Act of 2000
P.L. 110-385, Title II, Protecting Children in the 21st Century Act
18 USC 1460
18 USC 2246
18 USC 2256
20 USC 6777, 9134 (2003)
20 USC 6801 et seq., Part F, Elementary and Secondary Education Act of 1965, as amended (2003)
47 USC 254(h), (1), Communications Act of 1934, as amended (2003)

Students shall use Academy Information & Technology Resources (see definition Bylaw 0100) for educational purposes only. Academy Information & Technology Resources shall not be used for personal, non-~~school~~ academy related purposes. Use of Academy Information & Technology Resources is a privilege, not a right. When using Academy Information & Technology Resources, students must conduct themselves in a responsible, efficient, ethical, and legal manner. Students who engage ~~found to have engaged~~ in unauthorized or inappropriate use of Academy Information & Technology Resources, including any violation of these guidelines, may have their privilege limited or revoked, and may face further disciplinary action consistent with the Student Code of Conduct/Student Handbook~~,~~ and/or civil or criminal liability. Prior to accessing or using Academy Information & Technology Resources, students (eighteen (18) years of age and older) and parents of minor students must sign the Student Technology Acceptable Use and Safety Agreement (Form 7540.03 F1). Parents should discuss their values with their children and encourage students to make decisions regarding their use of Academy Information & Technology Resources that is in accord with their personal and family values, in addition to the Board of Directors standards. **( )** Students must complete a mandatory training session/program before using Academy Information & Technology Resources ~~being permitted to access or use Academy Technology Resources~~ **( )** and/or being assigned an ~~school~~ academy email address. **[END OF OPTION] [END OF OPTIONAL SENTENCE]**

This guideline also governs students' use of personally-owned ~~their personal~~ communication devices (PCD) (see definition Bylaw 0100) when the PCD's~~they~~ are connected to Academy Information & Technology Resources, or when used while the student is on Board-owned property or at a Board-sponsored activity.

~~-~~Below is a non-exhaustive list of unauthorized uses and prohibited behaviors. This guideline further provides a general overview of the responsibilities users assume when using Academy Information & Technology Resources.

A. All use of Academy Information & Technology Resources must be consistent with the educational mission and goals of the ~~School~~Academy.

B. Students may only access and use Academy Information & Technology Resources by using their assigned account **( )** and may only send Academy-related electronic communications using their Academy-assigned email addresses or services/apps connected/linked to their Academy-assigned e-mail addresses **[END OF OPTION]**. Use of another person's account/e-mail address is prohibited. Students may not allow other users to utilize their account/e-mail address and should not share their password or other multifactor authentication (MFA) device/app with other users. Students may not go beyond their authorized access. Students should take steps to prevent unauthorized access to their accounts by logging off or "locking" their ~~computers/laptops/tablets/personal communication devices when leaving them~~

~~unattended.~~ PCDs when leaving them unattended and employing MFA techniques whenever possible/available.

C. No user may access another person's ~~have access to another's~~ private files. Any attempt by users to access another user's or the Academy's non-public files, or phone or e-mail messages, is prohibited. ~~is considered theft.~~ Any attempts to gain access to unauthorized resources or data/information on Academy Information & Technology Resources ~~either on the Academy's computer or telephone systems or any systems to which the Academy has access~~ are prohibited. Similarly, students may not intentionally seek information on, obtain copies of, or modify files, data or passwords belonging to other users, or misrepresent other users on the Academy's Information & Technology Resources. ~~Network.~~

D. Students may not intentionally disable any security features used on Academy Information & Technology Resources.

E. Students may not use Academy Information & Technology Resources or their ~~personal communication device~~ PCDs to engage in vandalism, "hacking", or other illegal activities (e.g., software pirating; intellectual property violations; engaging in slander, libel, or harassment; threatening the life or safety of another; stalking; transmission of obscene materials or child pornography, including sexting; fraud; or sale of illegal substances and goods).

1. Slander and libel - In short, slander is "oral communication of false statements injurious to a person's reputation," and libel is "a false publication in writing, printing, or typewriting or in signs or pictures that maliciously damages a person's reputation or the act or an instance of presenting such a statement to the public." (The American Heritage Dictionary of the English Language. Third Edition is licensed from Houghton Mifflin Company. Copyright © 1992 by Houghton Mifflin Company. All rights reserved.) Students shall not knowingly or recklessly post/publish false or defamatory information about a person or organization. Students are reminded that material distributed over the Internet is "public" to a degree no other ~~school~~ academy publication or utterance is. As such, any remark may be seen by literally millions of people and harmful and false statements will be viewed in that light.

2. Students shall not use Academy Information & Technology Resources to transmit material that is threatening, obscene, disruptive, or sexually explicit or that can be construed as harassment or disparagement of others based upon their race, national origin, sex, (including sexual orientation or gender identity)~~sexual orientation or transgender identity,~~ marital status, age, disability, religion, or political beliefs. Sending, sharing, viewing, or possessing pictures, images, text messages, e-mails, or other materials of a sexual nature (e.g.,~~i.e.~~ sexting) in electronic or any other form, including the contents of a PCD~~personal communication device~~ or other electronic equipment, is grounds for discipline. Such actions will be reported to local law enforcement and child services as required by law.

3. Vandalism and Hacking – Deliberate attempts to damage the hardware, software, or information residing in Academy Information & Technology Resources or any services/apps ~~computer system~~ attached through the Internet are~~is~~ strictly prohibited. In particular, malicious use of Academy

Information & Technology Resources to develop programs that harass other users or infiltrate Academy Information & Technology Resources or PCDs and/or damage Academy Information & Technology Resources or PCDs ~~a computer/laptop/tablet or computer system and/or damage the software components of a computer or computing system~~ is prohibited.

Attempts to violate the integrity of private accounts, files, programs, or services/apps, deliberate infecting of Academy Information & Technology Resources or PCDs ~~or programs, the deliberate infecting of the network or computers, laptops, tablets, etc.,~~ attached to the network with a "virus", and/or attempts at hacking into any internal or external computer systems using any method will not be tolerated.

Students may not engage in vandalism or use Academy Information & Technology Resources or their personal communication devices in such a way that would disrupt others' use of Academy Information & Technology Resources.

Vandalism is defined as any malicious or intentional attempt to harm, steal, or destroy data /information of another user or Academy Information & Technology Resources. ~~of another user, school networks, or technology hardware.~~ This includes, but is not limited to, creating and/or uploading ~~or creation of~~ computer viruses, installing unapproved software, changing equipment configurations, deliberately destroying or stealing hardware and its components, or seeking to circumvent or bypass network security and/or the Board's technology protection measures. Students also must avoid intentionally wasting limited resources. Students must immediately notify ~~the~~ a teacher, Principal~~building principal~~, or _____ **[END OF OPTION]** if they identify a possible security problem. Students should not go looking for security problems, because this may be construed as an unlawful attempt to gain access.

CHOOSE OPTION #1 OR OPTION #2

[ ] OPTION # 1

4. Use of Academy Information & Technology Resources to access, process, distribute, display, or print child pornography and other material that is obscene, objectionable, inappropriate, and/or harmful to minors is prohibited. As such, the following material is prohibited: material that appeals to a prurient interest in nudity, sex, and excretion; material that 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 material that lacks serious literary, artistic, political, or scientific value as to minors. If a student inadvertently accesses material that is prohibited by this paragraph, ~~s/he~~the student should immediately disclose the inadvertent access to a teacher or Principal ~~the teacher or building principal~~. This will protect the user against an allegation that ~~s/he~~the user intentionally violated this provision.

[END OF OPTION #1]

[ ] OPTION # 2

4. Students shall not use Academy Information & Technology Resources to access, process, distribute, display, or print prohibited material at any time, for any purpose. Students may only access, process, distribute, display, or print restricted material, and/or limited access material as authorized below.

   a. Prohibited material includes material that constitutes child pornography and material that is obscene, objectionable, inappropriate, and/or harmful to minors, as defined by the Children's Internet Protection Act (CIPA). As such, the following material is prohibited: material that appeals to a prurient or unhealthy interest in nudity, sex, and excretion; material that 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 material that lacks serious literary, artistic, political, or scientific value as to minors. Prohibited material also includes material that appeals to a prurient or unhealthy interest in, or depicts, describes, or represents in a patently offensive way, violence, death, or bodily functions; material designated as for "adults" only; and material that promotes or advocates illegal activities.

   b. Restricted material may not be accessed by elementary or middle school students at any time, for any purpose. Restricted material may be accessed by high school students in the context of specific learning activities that have been approved by a teacher or staff member for legitimate research purposes. Materials that may arguably fall within the description provided for prohibited material that has clear educational relevance, such as material with literary, artistic, political, or scientific value, will be considered to be restricted. In addition, restricted material includes materials that promote or advocate the use of alcohol and tobacco, hate and discrimination, satanic and cult group membership, school cheating, and weapons. Sites that contain personal advertisements or facilitate making online connections with other people are restricted unless such sites have been specifically approved by the _____.

      [NOTE: THIS PARAGRAPH (b) CAN BE MODIFIED AS DESIRED BY THE ACADEMY.]

   c. Limited access material is material that is generally considered to be non-educational or entertainment. Limited access material may be accessed in the context of specific learning activities that are directed by a teacher or during periods that an ~~school~~ academy may designate as "open access" time. Limited access material includes such material as electronic commerce, games, jokes, recreation, entertainment, sports, and investment. **[NOTE: THIS LAST SENTENCE CAN BE MODIFIED AS DESIRED BY THE ACADEMY.]**

   If a student inadvertently accesses material that is considered prohibited or restricted, the student ~~s/he~~ should immediately disclose the inadvertent access to a teacher or Principal~~the teacher or building principal~~. This will

protect the student against an allegation that the student ~~s/he~~ intentionally violated the provision.

The determination of whether material is prohibited, restricted, or limited access shall be based on the content of the material and the intended use of the material, not on the protective actions of the technology protection measures. **( )** The fact that the technology protection measures have not protected against access to certain material shall not create the presumption that such material is appropriate for students to access. **[END OF OPTION]** The fact that the technology protection measures have blocked access to certain material shall not create the presumption that the material is inappropriate for students to access.

[END OF OPTION #2]

5. Unauthorized Use of Software or Other Intellectual Property from Any Source – All communications and information accessible via the Internet should be assumed to be private property (i.e., copyrighted and/or trademarked). Laws and ethics require proper handling of intellectual property. All copyright issues regarding software, information, and attributions/acknowledgement of authorship must be respected.

   Software is intellectual property~~,~~ and, with the exception of freeware, is illegal to use without legitimate license or permission from its creator or licensor. All software loaded on Academy Information & Technology Resources computers must be approved by the Technology Director, and the Academy must own or otherwise obtain, maintain, and retain the licenses for all copyrighted software loaded on Academy computers. Students are prohibited from using Academy Information & Technology Resources for the purpose of illegally copying another person's software. Illegal peer-to-peer file trafficking of copyrighted works is prohibited.

   Online articles, blog posts, podcasts, videos, and wiki entries are also intellectual property. Students should treat information found electronically in the same way they treat information found in printed sources – i.e., properly citing sources of information and refraining from plagiarism. Rules against plagiarism will be enforced.

F. Transmission of any material in violation of any State or Federal law or regulation, or Board policy is prohibited.

G. Students may not use Academy Information & Technology Resources ~~Academy Technology Resources may not be used~~ for private gain or commercial purposes (e.g., purchasing or offering for sale personal products or services by students), advertising, or political lobbying. **( )** This provision shall not limit the use of Academy Information & Technology Resources for the purpose of communicating with elected representatives or expressing views on political issues. **[This option is legally correct, but it need not be included.]**

H. Students may not use Academy Information & Technology ~~Use of Academy Technology~~ Resources to engage in cyberbullying ~~is prohibited~~. ""Cyberbullying" involves the use of information and communication technologies to support deliberate, repeated, and hostile behavior by an individual or group, which is

intended to harm others. [Bill Belsey (http//www.cyberbullying.org)] Cyberbullying may occur through e-mail, instant messaging (IM), chat room/Bash Boards, small text messages ~~text messages~~ (SMS), websites, voting booths, social media, and other technological means of communicating/publishing text, audios, and/or videos.

Cyberbullying includes, but is not limited to, the following:

1. posting/publishing slurs or rumors or other disparaging remarks about a student on a website or ~~on~~ weblog;

2. sending e-mails ~~e-mail~~ or instant messages that are mean or threatening~~,~~ or so numerous as to negatively impact the victim's use of that method of communication and/or drive up the victim's cell phone bill;

3. using or threatening to use a ~~camera~~ smartphone to take and/or send embarrassing and/or sexually explicit photographs/recordings of students;

4. posting/publishing online misleading or fake photographs of students. ~~on websites.~~

I. Students are expected to abide by the following generally-accepted rules of online etiquette:

1. Be polite, courteous, and respectful in your messages to others. Use language appropriate to ~~school~~ academy situations in any communications made through or utilizing Academy Information & Technology Resources. Do not use obscene, profane, lewd, vulgar, rude, inflammatory, sexually explicit, defamatory, threatening, abusive, or disrespectful language in communications made through or utilizing Academy Information & Technology Resources.

2. Do not engage in personal attacks, including prejudicial or discriminatory attacks.

3. Do not harass another person. Harassment is persistently acting in a manner that distresses or annoys another person. If a student is told by a person to stop sending that person ~~him/her~~ messages, the student must stop.

4. Do not post information that, if acted upon, could cause damage or a danger of disruption.

5. Never reveal names, addresses, phone numbers, or passwords of yourself or other students, family members, teachers, administrators, or other staff members while communicating on the Internet. This prohibition includes, but is not limited to, disclosing personally-identifiable~~personal identification~~ information on commercial websites.

6. Do not transmit to third parties/unknown individuals pictures or other information that could be used to establish ~~your~~ identity without prior approval of a teacher.

7. Never agree to get together with someone you "meet" online ~~on-line~~ without parent approval and participation.

8. Regularly check Academy-provided e-mail account and delete e-mails no longer needed.~~Check e-mail frequently and delete e-mail promptly.~~

9. Students should promptly disclose to a teacher or administrator any messages they receive that are inappropriate or make them feel uncomfortable, especially any e-mail that contains sexually explicit content (e.g. pornography). To aid in any investigation, students~~Students~~ should not delete such messages until instructed to do so by an administrator.

J. Downloading of files onto Academy Information & Technology Resources ~~Academy-owned equipment or contracted online educational services~~ is prohibited~~,~~ without prior approval from _____**.** If a student transfers files from online services/apps (e.g., electronic bulletin board services), ~~information services and electronic bulletin board services,~~ the student must check the file with a virus detection ~~virus-detection~~ program before opening the file for use. If a student transfers a file or installs a ~~software~~ program that infects the Academy's Information & Technology Resources with a virus and causes damage, the student will be liable for any and all repair costs ~~to make the Academy~~associated with making Academy Information & Technology Resources once again fully operational.

K. Students must secure prior approval from a teacher or the _____ before joining a Listserv (electronic mailing lists) and should not post personal messages on bulletin boards or "Listservs."

[CHOOSE OPTION #3 OR OPTION #4]

[ ] OPTION #3

L. Students are prohibited from accessing or participating in online "chat rooms" or other forms of direct electronic communication (e.g., instant messaging) (other than e-mail) without prior approval from a teacher or the _____. All such authorized communications must comply with these guidelines. Students may only use their ~~school~~academy-assigned accounts/e-mail~~email~~ addresses when accessing, using or participating in real-time electronic communications for education purposes.

[END OF OPTION #3]

[ ] OPTION #4

L. Students may use real-time electronic communication, such as chat or instant messaging, only under the direct supervision of a teacher or in moderated environments that have been established to support educational activities and have been approved by the Board, **[ ] School Leader ~~(employed by the Board~~ [ ] Educational Service Provider**, or Principal ~~building principal~~. Students may only use their Academy-assigned accounts/e-mail~~email~~ addresses when accessing, using or participating in real-time electronic communications for education purposes.

[END OF OPTION #4]

[CHOOSE OPTION #5 OR OPTION #6]

[ ] OPTION #5

M. Privacy in communication over the Internet through Academy Information & Technology Resources ~~the Academy's computer network~~ is not guaranteed. In order to verify compliance with these guidelines, the Board reserves the right to access,~~access~~ monitor, review, and inspect any directories, files and/or messages residing on or sent using ~~its~~ Academy Information & Technology Resources~~.~~. Messages relating to or in support of illegal activities will be reported to the appropriate authorities.

[END OF OPTION #5]

[ ] OPTION #6

M. Users have no right or expectation to privacy when using the Academy Information & Technology Resources. The Board reserves the right to access and inspect any facet of ~~its~~ Academy & Technology Resources, including, but not limited to, computers, laptops, tablets, and other devices, networks or Internet connections, online educational services, or apps, e-mail or other messaging or communication systems or any other electronic media within the Academy's ~~its~~ technology systems or that otherwise constitutes its property and any data, information, e-mail, communication, transmission, upload, download, message, or material of any nature or medium that may be contained therein. A student's use of Academy Information & Technology Resources constitutes ~~his/her~~the student's waiver of any right to privacy in anything ~~s/he~~the student creates, stores, sends, transmits, uploads, downloads, or receives on or through Academy Information &~~the~~ Technology Resources and related storage medium and equipment. Routine maintenance and monitoring, utilizing both technology monitoring systems and staff monitoring, may lead to the discovery that a user has violated Board policy/guidelines and/or the law. An individual search will be conducted if there is reasonable suspicion that a user has violated Board policy and/or law, or if requested by local, State, or Federal law enforcement officials. Students' parents have the right to request to see the contents of their children's files, e-mails, and records.

[END OF OPTION #6]

N. The following notice will be included as part of the computer log-on screen:

[CHOOSE EITHER OPTION #A OR OPTION #B]

[ ] OPTION #A

"Academy Information & Technology Resources (as defined in Bylaw 0100) are to be used for educational and professional purposes only. Users are reminded that

all use of Academy Information & Technology Resources, including Internet use, is monitored by the Academy and individual users have no expectation of privacy."

[END OF OPTION #A]

[ ] OPTION #B

NOTICE AND CONSENT FOR MONITORING

"Unauthorized or improper use of Academy Information & Technology Resources (as defined in Bylaw 0100) is strictly prohibited. Use of Academy Information & Technology Resources must comply with the Board's Technology Acceptable Use and Safety Policy/Agreement. Academy Information & Technology Resources are provided only for communication, processing, and storage of ~~school~~academy/education-related data/information and/or for authorized ~~School~~ academy use. Academy Information & Technology Resources are subject to monitoring for all lawful purposes (e.g., to ensure its proper functioning and management, to protect against improper or unauthorized use or access, and to verify the presence or performance of applicable security features or procedures and operational security) and individual users have no expectation of privacy.

Monitoring includes active attacks by authorized employees and/or agents of the Academy to test or verify the security of the system. During monitoring, data/information may be examined, recorded, copied, and/or used for authorized purposes. All data/information, including personal information, ~~placed~~ stored on or sent over the system may be monitored. Such monitoring may result in the acquisition, recording, and/or analysis of all data communicated, transmitted, processed, or stored in this system by a user. Unauthorized or inappropriate use may subject ~~you~~ the user to disciplinary action and/or criminal prosecution. Evidence of unauthorized or improper use collected during monitoring may be used for administrative, criminal, or other adverse action. Use of ~~this computer system,~~ Academy Information & Technology Resources, authorized or unauthorized, constitutes consent to monitoring for these purposes."

[END OF OPTION #B]

[END OF OPTIONS]

O. Use of the Internet and any data/information procured from the Internet is at the student's own risk. The Board makes no warranties of any kind, either express or implied, that the functions or ~~the~~ services provided by or through Academy Information & Technology Resources will be error-free or without defect. The Board is not responsible for any damage a user may suffer~~,~~ including, but not limited to, loss of data/information, service interruptions, or exposure to inappropriate material or people. The Board is not responsible for the accuracy or quality of data/information obtained through the Internet. Data/Information (including text, graphics, audio, video, etc.) from Internet sources used in student papers, reports, and projects must be cited the same as references to printed materials. The Board is not to be responsible for financial obligations arising through the unauthorized use of Academy Information & ~~its~~ Technology Resources. Students or parents of students will indemnify and hold the Board harmless from any losses sustained as the result of a student's misuse of Academy Information & Technology Resources.

P. Disclosure, use, and/or dissemination of personally identifiable information of minors via the Internet is prohibited, except as expressly authorized by the minor student's parent/guardian on the "Student Technology Acceptable Use and Safety Agreement Form." (See Form 7540.03F1).

( ) . Proprietary rights in the design of web sites, web pages, and services/apps hosted on Board-owned or Academy-affiliated servers remain ~~or leased servers remains~~ at all times with the Board. **[END OF OPTION]**

R. File-sharing is strictly prohibited. Students are prohibited from downloading and/or installing file-sharing software or programs on Academy Information & Technology Resources.

( ) Students may not use Academy Information & Technology Resources to establish or access web-based email accounts on commercial services (e.g., Gmail, iCloud, Outlook, Yahoo mail, etc.).

Students may not establish social media accounts on commercial services through the Ed-Tech (e.g., Facebook, Instagram, etc.) **[END OF OPTION]**

T. Since there is no central authority on the Internet, each site is responsible for its own users. Complaints received from other sites regarding any of the Academy's users will be fully investigated and disciplinary action will be ~~taken~~ imposed as appropriate.

U. Preservation of Resources and Priorities of Use: Academy Information & Technology Resources are limited. **( )** Because space on data storage devices ~~disk drives~~ and bandwidth across the lines that connect Academy Information & Technology Resources (both internally and externally) are limited, either programs nor data/information may be stored on the system without the permission of the _____.**[~~NOTE:~~ END OF OPTION]** Each student is permitted reasonable space to store email, web, and personal ~~school~~academy-related files. The Board reserves the right to require the purging of files in order to regain space on data storage devices ~~disk space~~. Students who require access to Academy Information & Technology Resources ~~for~~ class-or instruction-related activities have priority over other users. Students not using Academy Information & Technology Resources for class-related activities may be "bumped" by any student requiring access for a class- or instruction-related purpose. **[BEGIN OPTIONAL LANGUAGE] ( )** The following hierarchy will prevail in governing access to Academy Information & Technology Resources:

1. class work, assigned and supervised by a staff member.
2. class work, specifically assigned but independently conducted.
3. Personal correspondence (e-mail: ~~checking~~, composing, and sending).
4. Training (use of such programs as typing tutors, etc.).

5. Personal discovery ("surfing the Internet").

6. Other uses: access to resources for "other uses" may be further limited during the school day at the discretion of the Principal~~building principal~~ or _____ **[END OF OPTION]**.

Game playing is not permitted unless under the supervision of a teacher.

[END OF OPTIONAL LANGUAGE]

[ ] Artificial Intelligence/Natural Language Processing Tools: Absent express direction/permission from a teacher, a student may not use Artificial Intelligence (AI) or Natural Language Processing (NLP) tools to complete academy work (i.e., to create, compose, generate, or edit original content that they intend to submit as their own work). This prohibition includes, but is not limited to, the use of AI and NLP tools to prepare a writing assignment or creative art project or to answer questions on a quiz, test, or in-class or homework assignment. The preceding prohibition does not include and does not limit a student's use of AI/NLP tools that are features built into apps, including a word processing program, installed by the Academy on Academy-issued PCDs (e.g., Chromebooks), or AI/NLP tools that is/are listed as approved accommodation(s) or assistive technology pursuant to a student's individualized education program or Section 504 Plan. In particular, this prohibition does not include the use of speech-to-text features that are part of Academy-issued PCDs unless the purpose of the class work/assignment is to assess/test a student's knowledge of spelling, grammar, etc. If a student has any question(s) as to whether specific AI/NLP tools can be used for an assignment, the student should ask their teacher. If a student violates this prohibition, the student will be charged with plagiarism and disciplined in accordance with the Student Code of Conduct, including not receiving credit for the assignment.

Abuse of Network Resources

Peer-to-peer file sharing, mass mailings, and downloading of unauthorized games, videos, and music are wasteful of limited network resources and ~~are~~ forbidden. In addition, the unauthorized acquisition and sharing of copyrighted materials are~~is~~ illegal and unethical.

Unauthorized Printing

Academy printers may only be used to print ~~school~~academy-related documents and assignments. Printers, like other ~~school~~ academy resources, are to be used in a responsible manner. Ink cartridges and paper, along with printer repairs and replacement are very expensive. The Academy monitors printing by all users. Print jobs deemed excessive and abusive of this privilege may result in charges being assessed to the student. Users are prohibited from replacing ink cartridges and performing any other service or repairs to printers. Users should ask, as appropriate, for assistance to clear paper that is jamming a printer.

Any questions and concerns regarding these guidelines may be directed to _____.

REVISED GUIDELINE – SPRING 2023
STAFF TECHNOLOGY ACCEPTABLE USE AND SAFETY

Source P.L. 106-554, Children's Internet Protection Act of 2000
18 USC 1460
18 USC 2246
18 USC 2256
20 USC 6777, 9134 (2003)
20 USC 6801 et seq., Part F, Elementary and Secondary Education Act of 1965, as amended (2003)
47 USC 254(h), (1), Communications Act of 1934, as amended (2003)

Staff members shall use Academy Information & Technology Resources (see definition Bylaw 0100) for educational and professional purposes only.

[ ] Academy Information & Technology Resources (see definition Bylaw 0100) shall not be used for personal, nonwork~~non-work~~ related purposes.

[ ] Academy Information & Technology Resources (see definition Bylaw 0100) may be used for incidental personal, nonwork~~non-work~~ related purposes that do not interfere with the employee's performance of ~~his/her~~ job responsibilities, do not result in direct costs to the Academy, do not affect other users, use of the resources for education and work-related ~~work-related~~ purposes, do not expose the Academy to unnecessary risks, or violate applicable Board of Directors policies, administrative guidelines, or law/regulations.

Use of Academy Information & Technology Resources is a privilege, not a right. When using Academy Information & Technology Resources, staff members must conduct themselves in a responsible, efficient, ethical, and legal manner. Staff members found to have engaged in unauthorized or inappropriate use of Academy Information & Technology Resources ~~Technology and/or Information Resources~~, including any violation of these guidelines, may have their privilege limited or revoked, and may face further disciplinary action consistent with the applicable collective bargaining agreement, ~~and~~ Board policy, and/or civil or criminal liability. Prior to accessing or using Academy Information & Technology ~~Technology and/or Information~~ Resources, staff members must sign the Staff Technology Acceptable Use and Safety Agreement (Form 7540.04 F1). **( )** Staff members must complete a mandatory training session/program before being permitted to access or use Academy Information & Technology ~~Technology and/or Information~~ Resources and/or being assigned an ~~school~~ academy e-mail address. **[END OF OPTION]**

This guideline also governs staff members' use of personally-owned ~~their personal~~ communication devices (PCDs) (as defined in Bylaw 0100) when the PCDs ~~they~~ are connected to the Academy's Information & Technology Resources ~~Technology Resources, creating, using or transmitting Academy Information Resources,~~ or when used while the staff member is on Board-owned property or at a Board-sponsored activity. Staff are reminded that use of PCDs (including the sending of text messages) may generate a public or education record ~~or an education record~~ that needs to be maintained in accordance with the Board's record retention schedule, litigation hold, and/or Federal and State law.

Below is a non-exhaustive list of unauthorized uses and prohibited behaviors. This guideline further provides a general overview of the responsibilities users assume when using Academy Information & Technology Resources.~~Technology and/or Information Resources.~~

A. All use of Academy Information & Technology ~~the Academy Technology and/or Information~~ Resources must be consistent with the educational mission and goals of the Academy.

B. Staff members may only access and use Academy Information & Technology ~~Technology and/or Information~~ Resources by using their assigned account and may only send Academy-related electronic communications using their Academy-assigned email addresses or services/apps connected/linked to their Academy-assigned e-mail addresses. Use of another person's account/e-mail address is prohibited. Use of Educational Technology to access or use private e-mail accounts (e.g., G-mail, Yahoo Mail). Staff members may not allow other users to utilize their account/e-mail address and should not share their password or other multifactor authentication (MFA) device/app with other users. Staff members are expected to take steps to prevent unauthorized access to their accounts by logging off or "locking" their PCDs when leaving them unattended and employing MFA techniques whenever possible/available. ~~computers/laptops/tablets/personal communication devices when leaving them unattended.~~

C. No user may access another person's~~have access to another's~~ private files. Any attempt by users to access another user's or the Academy's non-public files, or phone or e-mail messages, is prohibited. ~~is considered theft.~~ Any attempts to gain access to unauthorized resources or data/information located on Academy Information & Technology Resources ~~either on the Academy's computer or telephone systems or any systems to which the Academy has access~~ are prohibited. Similarly, staff members may not intentionally seek data/information on or ~~on~~, obtain copies of~~of,~~ or modify files, data, or passwords belonging to other users ~~or persons,~~ or misrepresent other users on Academy Information & Technology Resources. ~~the Academy's network.~~

D. Staff members may not intentionally disable any security features used on Academy Information & Technology Resources.

E. Staff members may not use Academy Information & Technology Resources or their PCDs ~~personal communication devices~~ to engage in vandalism, "hacking", or other illegal activities (e.g., software pirating; intellectual property violations; engaging in slander, libel, or harassment; threatening the life or safety of another; stalking; transmission of obscene materials or child pornography, including sexting; fraud; and/or sale of illegal substances or goods).

1. Slander and libel - In short, slander is "oral communication of false statements injurious to a person's reputation," and libel is "a false publication in writing, printing, or typewriting, or in signs or pictures that maliciously damages a person's reputation or the public." (The American Heritage Dictionary of English Language Third Edition is licensed from Houghton Mifflin Company. Copyright © 1992 by Houghton Mifflin Company. All rights reserved.) Staff members shall not knowingly or recklessly post/publish false or defamatory information about a person or organization. Staff members are reminded that material distributed over the Internet is "public" to a degree no other ~~school~~ academy publication or utterance is. As such, any remark may be seen by literally millions of people and harmful and false statements will be viewed in that light.

2. Staff members shall not use Academy Information & Technology Resources to transmit material that is threatening, obscene, disruptive, or sexually explicit or that can be construed as harassment or disparagement of others based upon their race, national origin, sex (including sexual orientation or gender identity), ~~, sexual orientation or transgender identity,~~ marital status, age, disability, religion, or political beliefs. Sending, sharing, viewing, or possessing pictures, images, text messages, e-mails, or other materials of a sexual nature (e.g., ~~i.e.~~ sexting) in electronic or any other form, including the contents of a PCD ~~personal communication device~~ or other electronic equipment, is grounds for discipline up to and including termination. Such actions will be reported to local law enforcement and child services as required by law.

3. Vandalism and Hacking – Deliberate attempts to damage the hardware, software, or data/information residing in Academy Information & Technology Resources or any computer system attached through the Internet is strictly prohibited. In particular, malicious use of Academy Information & Technology Resources to develop programs that harass other users or infiltrate a computer/laptop/tablet or computer system and/or damage the software components of a computer or computing system is prohibited.

   Attempts to violate the integrity of private accounts, files, programs, or services/apps, the deliberate infecting of Academy Information & Technology Resources or PCDs ~~or programs, the deliberate infecting of the network or computers, laptops, tablets, etc.,~~ attached to the network with a "virus", and/or attempts at hacking into any internal or external computer systems using any method will not be tolerated.

   Staff members may not engage in vandalism or use Academy Information & Technology Resources or their PCDs~~personal communication devices~~ in such a way that would disrupt others' use of Academy Information & Technology Resources.~~technology resources.~~

   Vandalism is defined as any malicious or intentional attempt to harm, steal, or destroy data/information of another user of Academy Information & Technology Resources. ~~of another user, school networks, or technology hardware.~~ This includes, but is not limited to, creating and/or uploading ~~uploading or creation of~~ computer viruses, installing unapproved software, changing equipment configurations, deliberately destroying or stealing hardware and its components, or seeking to circumvent or bypass network security and/or the Board's technology protection measures. Staff members also must avoid intentionally wasting limited resources. Staff members must immediately notify the ~~Building~~ Principal or _____ if they identify a possible security problem. Staff members should not go looking for security problems, because this may be construed as an unlawful attempt to gain access.

[CHOOSE OPTION #1 OR OPTION #2]

[ ] OPTION #1

4. Use of Academy Information & Technology Resources to access, process, distribute, display, or print child pornography and other material that is

obscene, objectionable, inappropriate, and/or harmful to minors is prohibited. As such, the following material is prohibited: material that appeals to a prurient interest in nudity, sex, and excretion; material that 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 material that lacks serious literary, artistic, political, or scientific value as to minors. If a staff member inadvertently accesses material that is prohibited by this paragraph, ~~s/he~~the staff member should immediately disclose the inadvertent access to the Building Principal or _____. This will protect the user against an allegation that ~~s/he~~the user intentionally violated this provision.

[END OF OPTION #1]

[ ] OPTION # 2

4. Staff members shall not use Academy Information & Technology Resources to access, process, distribute, display, or print prohibited material at any time, for any purpose. Staff members may only access, process, distribute, display, or print restricted material, and/or limited access material as authorized below.

   a. Prohibited material includes material that constitutes child pornography and material that is obscene, objectionable, inappropriate, and/or harmful to minors, as defined by the Children's Internet Protection Act (CIPA). As such, the following material is prohibited: material that appeals to a prurient or unhealthy interest in nudity, sex, and excretion; material that 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 material that lacks serious literary, artistic, political, or scientific value as to minors. Prohibited material also includes material that appeals to a prurient or unhealthy interest in, or depicts, describes, or represents in a patently offensive way, violence, death, or bodily functions; material designated as for "adults" only; and material that promotes or advocates illegal activities.

   b. Restricted material may be accessed by staff members in the context of specific learning activities for legitimate research and professional development purposes. Materials that may arguably fall within the description provided for prohibited material that has clear educational relevance, such as materials with literary, artistic, political, or scientific value, will be considered to be restricted. In addition, restricted material includes materials that promote or advocate the use of alcohol and tobacco, hate and discrimination, satanic and cult group membership, school cheating, and weapons. Sites that contain personal advertisements or facilitate making online connections with other people are restricted unless such sites have been specifically approved by the _____. **[NOTE: THIS PARAGRAPH CAN BE MODIFIED AS DESIRED BY THE ACADEMY.]**

c. Limited access material is material that is generally considered to be non-educational or entertainment. Limited access material may be accessed in the context of specific learning activities or during nonwork ~~non-work~~ times. Limited access material includes such material as electronic commerce, games, jokes, recreation, entertainment, sports, and investment. **[NOTE: THIS LAST SENTENCE CAN BE MODIFIED AS DESIRED BY THE ACADEMY.]**

If a staff member inadvertently accesses material that is considered prohibited or restricted, ~~s/he~~ should immediately disclose the inadvertent access to the ~~Building~~ Principal or _____. This will protect the staff member against an allegation that ~~s/he~~the staff member intentionally violated the provision.

The determination of whether material is prohibited, restricted, or limited access shall be based on the content of the material and the intended use of the material, not on the protective actions of the technology protection measures. **( )** The fact that the technology protection measures have not protected against access to certain material shall not create the presumption that such material is appropriate for ~~students~~ staff members to access. **[END OF OPTIONAL SENTENCE]** The fact that the technology protection measures have blocked access to certain material shall not create the presumption that the material is inappropriate for staff members to access.

[END OF OPTION #2]

5. Unauthorized Use of Software or Other Intellectual Property from Any Source – Laws and ethics require proper handling of intellectual property. Software is intellectual property~~,~~ and, with the exception of freeware, is illegal to use without legitimate license or permission from the software's~~its~~ creator or licensor. All software loaded on Academy Information & Technology Resources ~~computers~~ must be approved by the Director of Technology, and the Academy must own or otherwise obtain, maintain, and retain the licenses for all copyrighted software loaded on Academy Information & Technology Resources. ~~computers.~~ Staff members are prohibited from using Academy Information & Technology Resources for the purpose of illegally copying another person's software. Illegal peer-to-peer file trafficking of copyrighted works is prohibited.

   Online articles, blog posts, podcasts, videos, and wiki entries are also intellectual property. Staff members should treat information found electronically in the same way they treat information found in printed sources – i.e., properly citing sources of information and refraining from plagiarism.

F. Transmission of any material in violation of any State or Federal law or regulation~~,~~ or Board policy is prohibited.

G. Staff members may not use Academy Information & Technology Resources ~~Academy Technology Resources may not be used~~ for private gain or commercial purposes (e.g., purchasing or offering for sale personal products or services by staff members), advertising, or political lobbying or campaigning. ~~is prohibited.~~ **[NOTE: THE BOARD COULD ALLOW LIMITED COMMERCIAL ACTIVITY BY STAFF**

MEMBERS; (e.g., sale of one (1) of a kind items on staff intranet)] ( ) This provision shall not limit the use of Academy Information & Technology Resources by staff members for the purpose of communicating with elected representatives or expressing views on political issues. **[NOTE: This option is legally correct, but it need not be included.]** ( ) Staff members may use Academy Information & Technology Resources for communication related to collective bargaining and union organizational activities. **[NOTE: THIS OPTION IS SUBJECT TO BARGAINING.]**

H. Staff members are expected to abide by the following generally accepted rules of online etiquette:

1. Be polite, courteous, and respectful in your messages to others. Use language appropriate to ~~school~~ academy situations in any communications made through or utilizing Academy Information & Technology Resources. Do not use obscene, profane, lewd, vulgar, rude, inflammatory, sexually explicit, defamatory, threatening, abusive, or disrespectful language in communications made through or utilizing Academy Information & Technology Resources (including, but not limited to, public messages, private messages, and material posted on webpages).

2. Do not engage in personal attacks, including prejudicial or discriminatory attacks.

3. Do not harass another person. Harassment is persistently acting in a manner that distresses or annoys another person. If a staff member is told by a person to stop sending ~~him/her~~them messages, the staff member must stop.

4. Do not post information that, if acted upon, could cause damage or a danger of disruption.

5. Never reveal names, addresses, phone numbers, passwords or other personal information of students while communicating on the Internet~~,~~ unless there is prior written approval from a student (who is eighteen (18) years of age or older) or a parent/guardian of a minor student (who is seventeen (17) years of age or younger) ~~parental approval~~ or it is otherwise permitted by Federal and/or State law.

6. Regularly check Academy-provided e-mail account and delete e-mails no longer needed. Nothing herein alters the staff member's responsibility to preserve e-mail and other electronically stored information that constitutes a public record, a student education record, and/or a record subject to a Litigation Hold.

I. All communications and information accessible via the Internet should be assumed to be private property (i.e, copyrighted and/or trademarked). All copyright issues regarding software, information, and attributions/acknowledgment of authorship must be respected.

J. Saving or otherwise specifically downloading files, from the Internet or otherwise unauthorized places, onto the Academy-owned equipment or contracted online educational services is prohibited, without prior approval from _____. If a staff member transfers files from information services

and/or electronic bulletin board services, the staff member must check the file with a virus detection ~~virus-detection~~ program before opening the file for use. Only public domain software may be downloaded. If a staff member transfers a file or installs a software program that infects Academy Information & Technology Resources y with a virus and causes damage, the staff member will be liable for any and all repair costs to make the Academy Information & Technology Resources~~Education Technology~~ once again fully operational.

[CHOOSE OPTION #3 OR OPTION #4]

[ ] OPTION #3

K. Privacy in communication over the Internet and through the Academy's Information & Technology Resources ~~computer network~~ is not guaranteed. In order to verify compliance with these guidelines, the Board reserves the right to access, monitor, review and inspect any directories, files and/or messages stored on or sent/received using ~~its~~ Academy Information & Technology Resources. All Staff members should assume that all messages and communications are being monitored, reviewed, and inspected. Messages relating to or in support of illegal activities will be reported to the appropriate authorities.

[END OF OPTION #3]

[ ] OPTION #4

K. Users have no right or expectation to privacy when using Academy Information & Technology ~~and/or Information~~ Resources. The Board reserves the right to access, monitor, and inspect any facet of its Academy Information & Technology Resources ~~Technology and/or Information Resources,~~ including, but not limited to, computers, laptops, tablets, and other web-enabled devices, networks or Internet connections or online educational services or apps, e-mail or other messaging or communication systems, or any other electronic media within its technology systems or that otherwise constitutes its property, and any data, information, e-mail, communication, transmission, upload, download, message, or material of any nature or medium that may be contained therein. A staff member's use of Academy Information & Technology Resources constitutes the staff member's ~~Technology and/or Information Resources constitutes his/her~~ waiver of any right to privacy in anything ~~s/he~~the staff member creates, stores, sends, transmits, uploads, downloads, or receives on or through ~~the~~ Academy Information & Technology Resources and related storage medium and equipment. Routine maintenance and monitoring, utilizing both technology monitoring systems and staff monitoring, may lead to a discovery that a staff member has violated Board policy and/or the law. An individual search will be conducted if there is reasonable suspicion that a staff member has violated Board policy/guidelines and/or law, or if requested by local, State or Federal law enforcement officials. Staff are reminded that their communications are subject to Michigan's public records laws and FERPA/State law.

[END OF OPTION #4]

[CHOOSE OPTION #A OR OPTION #B]

The following Notice will be included as part of the computer log-on screen:

[ ] [OPTION #A]

"Academy Information & Technology Resources (as defined in Bylaw 0100) ~~Technology Resources (including computers, laptops, tablets, e-readers, cellular/mobile telephones, smartphones, other web-enabled devices, video and/or audio recording equipment, projectors, software and operating systems that work on any device, copy machines, printers and scanners, information storage devices (including mobile/portable storage devices such as external hard drives, CDs/DVDs, USB thumb drives and memory chips), the computer network, Internet connection, and online educational services and apps)~~ are to be used for educational and professional purposes only. Users are reminded that all use of Academy Information & Technology Resources, including Internet use, is monitored by the Academy and individual users have no expectation of privacy."

[END OF OPTION #A]

[ ] [OPTION #B]

NOTICE AND CONSENT FOR MONITORING

"Unauthorized or improper use of Academy Information & Technology Resources (as defined in Bylaw 0100) is strictly prohibited. Use of Academy Information & Technology Resources ~~Technology Recourses is strictly prohibited. Use of Academy Technology Resources, including its computers, laptops, tablets, e-readers, cellular/mobile telephones, smartphones, other web-enabled devices, video and/or audio recording equipment, projectors, software and operating systems that work on any device, copy machines, printers and scanners, information storage devices (including mobile/portable storage devices such as external hard drivers, CDs/DVDs, USB thumb drives and memory chips), the computer network, and Internet connection, and online educational services and apps,~~ must comply with the Board's Technology Acceptable Use and Safety Policy/Agreement. Academy Information & Technology Resources are provided only for communication, processing, and storage of ~~school~~academy/education related information and/or for authorized Academy use. Academy Information & Technology Resources are subject to monitoring for all lawful purposes, (e.g., to ensure its proper functioning and management, to protect against improper or unauthorized use or access, and to verify the presence or performance of applicable security features or procedures and operational security) and individual users have no expectation of privacy.

Monitoring includes active attacks by authorized employees and/or agents of the Academy to test or verify the security of the system. During monitoring, data/information may be examined, recorded, copied, and/or used for authorized purposes. All data/information, including personal information, stored on or transmitted through the system may be monitored. Such monitoring may result in the acquisition, recording, and/or analysis of all data/information communicated, transmitted, processed, or stored in this system by a user. Unauthorized or inappropriate use may subject ~~you~~ the user to disciplinary action and/or criminal prosecution. Evidence of unauthorized or improper use collected during monitoring may be used for administrative, criminal, or other adverse action. Use

of Academy Information & Technology Resources, ~~this computer system,~~ authorized or unauthorized, constitutes consent to monitoring for these purposes."

[END OF OPTION #B]

L. Use of the Internet and any data/information procured from the Internet is at the staff member's own risk. The Board makes no warranties of any kind, either express or implied, that the functions or the services provided by or through Academy Information & Technology Resources will be error-free or without defect. The Board is not responsible for any damage a user may suffer~~,~~ including, but not limited to, loss of data , service interruptions, or exposure to inappropriate material or people. The Board is not responsible for the accuracy or quality of information obtained through the Internet. Information (including text, graphics, audio, video, etc.) from Internet sources used in class must be cited the same as references to printed materials. The Board is not responsible for financial obligations arising through the unauthorized use of ~~its~~ Academy Information & Technology Resources. Staff members will indemnify and hold the Board harmless from any losses sustained as the result of the staff member's misuse of the Academy Information & Technology Resources.

M. Disclosure, use, and/or dissemination of personally identifiable information of minors via the Internet is prohibited, except as expressly authorized by the minor student's parent/guardian on the "Student Technology Acceptable Use and Safety Agreement Form." (See Form 7540.01 F1)

[CHOOSE OPTION #5 OR OPTION #6]

[ ] [OPTION #5]

N. Proprietary rights in the design of websites, web pages, and services/apps ~~web sites/services/apps~~ hosted on Board-owned or Academy-affiliated servers remain ~~leased servers remains~~ at all times with the Board without prior written authorization.

[END OF OPTION #5]

[ ] [OPTION #6]

N. Staff members own the copyright to works created outside the scope of their employment responsibilities and without the use of Board resources. Staff members may post/publish such work on the Academy website and/or intranet to facilitate access by students and/or staff. Notice of such posting/publishing and claim of ownership must be provided to the ~~Building~~ Principal or _____. By posting/publishing such work on the Academy's website and/or intranet, the staff member agrees to grant a non-exclusive license or permission for any staff or student within the Academy to freely use such work. The Board shall own the copyright on any works created by staff members within the scope of their employment responsibilities.

[END OF OPTION #6]

O. Staff members are reminded that student personally identifiable information is confidential and may not be disclosed without prior written permission from a student

(eighteen (18) years of age or older) or the parent/guardian of a minor student (seventeen (17) years of age or younger).~~parental permission.~~

P. File-sharing is strictly prohibited. Staff members are prohibited from downloading and/or installing file-sharing software of programs on Academy Information & Technology Resources.

[ ] Staff members may not use Academy Information & Technology Resources to establish or access web-based email accounts on commercial services (e.g., Gmail, iCloud, Outlook, Yahoo mail, etc.).

Staff members may not use Academy Information & Technology Resources to establish or access social media accounts on commercial services (e.g., Facebook, Instagram, etc.) **[END OF OPTION]**

Q. Since there is no central authority on the Internet, each site is responsible for its own users. Complaints received from other sites regarding any of the Academy's users will be fully investigated and disciplinary action will be ~~taken~~ imposed as appropriate.

R. Preservation of Resources: Academy Information & Technology Resources are limited. **( )** Because space on disk drives and bandwidth across the wires that connect Academy Information Technology Resources (both internally and externally) are limited, neither programs nor information may be stored on the system without the permission of the **_____**. **[~~NOTE:~~ END OF OPTION]** Each staff member is permitted reasonable space to store email, web, and personal academy/work-related ~~school/work related~~ files. The Board reserves the right to require the purging of files in order to regain space on the data storage devices.~~disk space.~~

[ ] Staff members are **( )** required **( )** encouraged **[END OF OPTION]** to limit student exposure to commercial advertising and product promotion when selecting/developing ~~the~~ Academy or classroom websites, web pages, or services/apps~~/services/apps~~ or giving other assignments that utilize the Internet. Under all circumstances, staff members must comply with the Children's Online Privacy Protection Act of 1998 (COPPA), 15 U.S.C. § § 6501-6506.

1. Websites with extensive commercial advertising may be included on ~~the~~ Academy or classroom websites, web pages, and/or services/apps ~~websites/services/apps~~ or designated as a required or recommended site only if there is a compelling educational reason for such selection.

2. Staff members may make use of high-quality, unbiased online educational materials that have been produced with corporate sponsorship. Staff members may not make use of educational materials that have been developed primarily for the purpose of promoting a company and/or its products or services.

[END OF OPTION]

Abuse of Network Resources

Peer-to-peer file sharing, mass mailings, and downloading of unauthorized games, videos, and music are wasteful of limited network resources and are forbidden. In addition, the unauthorized acquisition and sharing of copyrighted materials is illegal and unethical.

Unauthorized Printing

Academy printers may only be used to print ~~school~~academy/work-related documents. Printers, like other ~~school~~ academy resources, are to be used in a responsible manner. Ink cartridges and paper, along with printer repairs and replacement are very expensive. The Academy monitors printing by a user. Print jobs deemed excessive and abusive of this privilege may result in charges being assessed to the staff member.

Any questions and concerns regarding these guidelines may be directed to _____.

REVISED GUIDELINE – SPRING 2023
CONTINUITY OF ORGANIZATIONAL OPERATIONS PLAN

Since continuity ~~Continuity~~ planning is based on the assumption that the Academy will not have advanced ~~necessarily receive~~ warning of an impending emergency, it is essential that the Administration conduct a risk assessment to identify potential areas of risk and vulnerability so a continuity of organizational operations plan can be developed and put in place to eliminate or at least mitigate/reduce the potential impact of an event. ~~As a result, a risk assessment is essential to continuity planning and is conducted to identify potential areas of risk and vulnerability and to put plans in place to mitigate by eliminating or reducing the potential impact of an event.~~ Continuity management consists of the organizational decisions, processes, and tools that are created and practiced in advance to address as many of the foreseeable circumstances that might arise and impact the Academy in the aftermath of a disaster. ~~put in place in advance to handle the aftermath of a disaster that impacts the Academy.~~

A crisis or emergency might affect the Academy only, or be part of a local, regional, or national event. This guideline provides structure to the continuity management strategy, but the overall plan should be much more comprehensive and include, at the minimum, the following elements:

Plan Outline

A. Delineation of the critical operations, management, and administrative functions that are essential for the Academy to fulfill its educational mission and carry out its business operations. ~~those functions that are essential for the Academy to perform critical operational, management, and administrative functions and that enable staff to provide access to curricular materials and other online resources for their students.~~

B. Assumptions and constraints inherent in ~~from~~ the planning process.

C. Detailed communications~~Communications~~ plan both internal to Academy and with external agencies and constituents.

D. Decision process and authority for activation.

E. Staff roster/directory, including multiple means of contact.

F. Procedures to enable readiness – risk assessment, location of all critical documents, and data and infrastructure resources.

G. Development and implementation of procedures and plans to mitigate risks.

H. Provisions for personnel training and accountability.

I. Reliable sources and processes to acquire additional resources to sustain operations for thirty (30) days.

J. Plan Contents

1. Include purpose, objectives, applicability, and scope, and authorities and references.

2. Describe the concept of operations and ~~contain~~specify:

   a. key staff: incident management team, assessment teams;

   b. mission essential functions: communications, vital records, ~~technology hardware/network connectivity/data,~~ Academy Information & Technology Resources, and facilities/relocation sites;

   c. direction and control;

   d. alert and notification;

   e. procedures for documentation of expenses and impact to facilitate recovery of costs. ~~impact for recovery of cost.~~

3. List personnel responsibilities and procedures, team assignments.

4. Outline phases (activation, alternate operations, reconstitution & termination).

5. Provide detailed information on each of the essential elements.

6. Implementation mechanisms, depending upon the magnitude of the incident.

Plan Execution

Activation (zero (0) - twenty-four (24) hours)

A. Alert and notification procedures, call trees.

B. Initial actions.

C. Evacuation, shelter, lockdown procedures.

D. Activation protocols/~~-~~procedures – during regular business hours and when the Academy offices/buildings are closed to the public.~~duty hours and during non-duty hours.~~

E. Deployment and department procedures for damage assessment - time-phased operations.

F. Transition to alternate operational sites and systems.

G. Site support responsibilities.

Alternate Operations Sites (twenty-four (24) hours to Termination – up to thirty (30) days)

A. Execution of mission essential functions.

B. Establishment of communications.

C. Staff contingency responsibilities.~~Contingency staff responsibilities.~~

D. Augmentation of staff.

E. Provision of guidance to essential and non-essential personnel.

F. Development of plans and schedules for reconstitution and termination (and return to normal operations).

G. Offsite recovery mechanisms for essential operational functions and Academy mission.

Reconstitution and Termination (Cessation of Disaster Recovery Alternative Site/Return to Normal Operations)

A. Overview.

B. Procedures.

C. After action review and remedial action plans.

Management and maintenance of the Academy's Continuity of Organizational Operations Plan (COOP) is a comprehensive task that depends on a multi-disciplinary team. The Academy's Continuity Management Team should be composed of upper-level managers in the Academy administration that represent all key functional areas and staff representatives from key departments and school site(s). ~~representatives from key departmental and school site faculty and staff.~~ These areas may include but not be limited to, the following departments/divisions:

( ) Operations and Systems

( ) Safety and Security

( ) Technology

( ) Maintenance/Construction

( ) Risk Management

( ) Legal Affairs

( ) Public Relations

( ) Personnel/Human Resources

( ) Finance/Payroll

( ) Purchasing

( ) Transportation

( ) Food Service

( ) ~~School~~ Academy Administration

( ) Teaching and Learning

( ) Student Services

( ) _____ [other]

( ) _____ [other]

REVISED GUIDELINE – SPRING 2023
COLLECTION, CLASSIFICATION, RETENTION, ACCESS AND SECURITY OF ACADEMY DATA/INFORMATION

Academy Information & Technology Resources (see definition in Bylaw 0100) are some of the most valuable assets owned by an Academy. An Academy produces, collects, and uses many different types of data/information in fulfilling its mission. Laws and Board of Directors policy mandate confidentiality and protection of certain types of data/information. Academy data/information shall be classified as Confidential, Controlled, or Published. Data/information will be considered Controlled until identified otherwise.

This administrative guideline aims to ~~procedure will~~ help Academy employees to classify any data/information created, stored, or transmitted by the Academy for the purposes of determining the level of protection required and applicable policies and laws.

This ~~procedure~~ guideline applies to all types of data/information:

A. Electronic data/information.

B. Data/information recorded on paper.

C. Data/information shared orally, visually, or by other means.

For purposes of this procedure, "Published Data/Information" means data/information made available to the public through posting to public websites, or distribution through e-mail, social media, print publications, or other media. This includes data/information that can be disclosed without restriction, such as unrestricted directory information, Academy maps, syllabi and course materials, and meeting minutes.

“Controlled Data/Information” means data/information that is not generally created or made available for public consumption, but may be subject to release through a public records request or pursuant to another State or Federal law. This includes operational/business records, select personnel information (e.g., employees’ salaries), Academy expenditures, and internal communications that do not contain Confidential Data/Information.

“Confidential Data/Information” means data/information that is exempt or must be protected from unauthorized disclosure or public release based on State and/or Federal laws or regulations or applicable legal agreements. This includes “protected health information” covered by HIPAA, student records as defined by FERPA and State law, Social Security numbers, credit/debit card information, security records, personal employee information, critical infrastructure information (e.g., physical plant detail, IT systems information, system passwords, security plans, etc.) and documents protected by attorney-client privilege.

Below is a summary of the minimum standard protection requirements for each category of data/information when being used or handled in a specific context (e.g., Confidential Data/Information sent in an e-mail message). These protection standards do not ~~are not intended to~~ supersede any regulatory or contractual requirements for handling data/information. Some specific data/information sets, such as student records data/information, credit/debit card data/information, healthcare data/information, and financial

accounting data/information may have stricter requirements in addition to the minimum standard requirements listed below.

Published Data/Information:

When it comes to Published Data/Information, there are no protection requirements when it comes to:

A. collecting/using it;

B. granting access or sharing it, including disclosing it, publicly posting/publishing it, or electronically displaying it;

C. exchanging it with third parties, services providers, cloud services, etc.;

D. storing it on removable media (e.g., thumb drives, CDs, tapes, etc.);

E. electronically transmitting it, including e-mailing it or sending it via other electronic messaging services/~~platforms~~apps;

F. printing, mailing or faxing it; and

G. disposing of it (subject to the Academy's record retention policy, a litigation hold, and administrative guidelines).

With respect to public records requests, Published Data/Information can be readily provided upon request; however, individuals who receive a request must coordinate with Academy administration before providing the information.

When Published Data/Information is stored or processed in a server environment, and the server is connected to the Academy's network, the server must comply with Minimum Security Standards for Networked Devices. This requirement also applies to Published Data/Information stored in the cloud (e.g., OneDrive, Google Drive, Dropbox, etc.).

When Published Data/Information is stored or processed in an endpoint environment (e.g., a personal communication device (PCD) (as defined in Bylaw 0100)), ~~laptop, smartphone, desktop computer, tablet, etc.),~~ the endpoint device if connected to the Academy's network, must comply with Minimum Security Standards for Networked Devices.

Controlled Data/Information:

When it comes to Controlled Data/Information, there are no protection requirements when it comes to:

A. collecting or using it;

B. storing it on removable media (e.g., thumb drives, CDs, tapes, etc.);

C. electronically transmitting it, including e-mailing it or sending it via other electronic messaging services/~~platforms~~apps, except reasonable methods shall be used to ensure Controlled Data/Information is only included in

messages to authorized individuals or individuals with legitimate need-to-know access ~~need to know~~;

D. disposing of it (subject to the Academy's record retention policy, a litigation hold, and administrative guidelines).

When it comes to Controlled Data/Information, reasonable methods must be used to ensure only authorized individuals or individuals with ~~a~~ legitimate need-to-know access ~~or~~ shared it. Further, reasonable methods must be used to ensure Controlled Data/Information is only disclosed or electronically displayed to authorized individuals or individuals with legitimate need-to-know access.

When it comes to storing, transmitting and retrieving Controlled Data/Information with or utilizing third party service providers, cloud services, etc., reasonable methods must be used to ensure the third parties' responsibilities for confidentiality/privacy of the data/information are defined and documented.

Printed materials, including those being mailed or faxed, that contain Controlled Data/Information must be distributed or made available only to authorized individuals or individuals with legitimate need-to-know access.

Individuals who receive public records requests involving Controlled Data/Information must coordinate with Academy administration before providing the requested data/information.

When Controlled Data/Information is stored or processed in a server environment, and the server is connected to the Academy's network, the server must comply with Minimum Security Standards for Networked Devices. This requirement also applies to Controlled Data/Information stored in the cloud (e.g., OneDrive, Google Drive, Dropbox, etc.).

When Controlled Data/Information is stored or processed in an endpoint environment (e.g., a PCD), ~~laptop, smartphone, desktop computer, tablet, etc.),~~ the endpoint device if connected to the Academy's network must comply with Minimum Security Standards for Networked Devices.

Confidential Data/Information:

When it comes to Confidential Data/Information, its collection and use are~~is~~ limited to authorized purposes as outlined in the Academy's privacy policy. Departments or schools that collect and/or use Confidential Data/Information must use Academy-provided or approved servers, devices, systems, and/or processes to handle this type of data/information.

[ ] If feasible, Academy web pages that are used to collect Confidential Data/Information will include a link to the Academy's privacy policy.

Social Security numbers (SSNs) shall not be used to identify members of the Academy's community if there are reasonable alternatives. SSNs shall not be used as a username or a password.

When it comes to Confidential Data/Information, access shall be limited to authorized Academy officials or agents with a legitimate academic or business interest and a need-to-know as outlined in the Board's privacy policy. All access shall be approved by an

appropriate administrator **( )** and tracked in a manner that can be audited **[END OF OPTION]**. Before granting access to or exchanging Confidential Data/Information with third parties, service providers, cloud services, etc., contractual agreements that outline security responsibilities shall be in place and approved by the Board's legal counsel.

Confidential Data/Information may not be disclosed without appropriate consent or unless required by law. Confidential Data/Information shall not be posted publicly; directory information, however, can be disclosed without consent, unless a student/parent opts out of the directory information disclosure.

Confidential Data/Information shall be displayed only to authorized and authenticated users of the Academy system, and~~,~~ where possible, identifying numbers or account numbers shall be, at least partially, masked or redacted.

Confidential Data/Information is typically not subject to release pursuant to a public records request. However, some public records requests may be fulfilled by redacting Confidential Data/Information in the record. Individuals who receive such requests must coordinate with Academy administration before responding to the request.

When Confidential Data/Information is stored or processed in a server environment, the server must comply with Minimum Security Standards for Confidential Devices. This requirement also applies to Controlled Data/Information stored in the cloud (e.g., OneDrive, Google Drive, Dropbox, etc.).

When Confidential Data/Information is stored or processed in an endpoint environment (e.g., PCD), ~~laptop, smartphone, desktop computer, tablet, etc.),~~ the endpoint device, if connected to the Academy's network must comply with Minimum Security Standards for Networked Devices.

Storing credit/debit card data/information on servers or endpoint devices is not permitted.

Storing Confidential Data/Information on PCDs ~~personal communication devices~~ is not permitted~~,~~ unless expressly authorized by the **[ ] Board [ ] School Leader ~~(employed by the Board)~~ [ ] Educational Service Provider** and stored in an encrypted file format, and the device automatically ~~secure~~ and securely locks when not in use.

[DRAFTING NOTE: SELECT OPTION #1 OR OPTION #2]

[ ] [OPTION #1]

Unless expressly authorized by the **[ ] Board [ ] School Leader ~~(employed by the Board)~~ [ ] Educational Service Provider**, Confidential Data/Information shall not be stored on removable media (e.g., thumb drives, CDs, tapes, etc.). Further, it~~It~~ is to be stored in an encrypted file format or within an encrypted volume, and media is to be stored in a physically secure environment, and the media is owned by the Academy.

[END OF OPTION #1]

[ ] [OPTION #2]

Storing of Confidential Data/Information is only allowed on Academy-approved devices/systems that are adequate to protect that data (i.e., secure and encrypted).

[END OF OPTION #2]

Confidential Data/Information may only be electronically transmitted if it is in an encrypted file format or over a secure protocol or secure, authenticated connection. Confidential Data/Information may only be transmitted via e-mail or other electronic messaging service/platform if the data/information is contained within an encrypted/password-protected~~password protected~~ file attachment. Such messages may only be sent to authorized individuals or other individuals with a legitimate need-to-know.

Printed materials, including those being mailed or faxed, that contain Confidential Data/Information must be distributed or made available only to authorized individuals or individuals with legitimate need-to-know. Access to any area where printed records containing Confidential Data/Information are stored shall be limited by use of controls (e.g., locks, doors, monitoring, etc.) sufficient to prevent unauthorized entry.

SSNs shall not be printed on any card required to access services.

When ready for disposal, Confidential Data/Information shall be deleted and unrecoverable. Physical media (e.g., paper, CDs, tapes, etc.) should be destroyed so that Confidential Data/Information on the media cannot be recovered or reconstructed. All disposals must be consistent with State law.

The following are required:

A. enforcement of this procedure throughout the Academy;

B. a periodic assessment of risk on the procedure;

C. training about classification, retention, access, and security of all Academy data/information;

D. internal controls related to classification, retention, access, and security of all Academy data/information;

( ) developing procedures for dealing with unauthorized release of Academy Confidential Data/Information (See AG 8305C).

Each Academy department is responsible for implementing, reviewing and monitoring internal policies, practices, etc., to assure compliance with this ~~procedure~~guideline.

All procedures shall be consistent with public records laws and records retention plans and schedules as required by State and Federal laws and regulations.

Noncompliance with these standards may incur the same types of disciplinary measures and consequences as violations of other Board policies, including progressive discipline, up to and including termination of employment~~,~~ or, in the cases where students are involved, reporting of a Student Code of Conduct violation~~,~~ or referral to law enforcement.

Any device that does not meet the minimum security requirements outlined in this standard ~~may~~ must be removed from the Academy's business network, disabled, etc., as appropriate until the device can comply with this standard.

Exceptions may be granted in cases where security risks are mitigated by alternative methods~~,~~ or in cases where security risks are at a low, acceptable level and compliance with minimum security requirements would interfere with legitimate academic or business needs. To request a security exception, contact the Academy's Director of Information Technology.

REVISED GUIDELINE – SPRING 2023
INFORMATION SECURITY RESPONSIBILITIES

The Academy collects and maintains large amounts of data/information that must be protected and preserved.

To strengthen security of Academy Information & Technology Resources (see definition Bylaw 0100) ~~and Information Resources (see definition Bylaw 0100)~~, the Academy has developed a series of information security policies available through the Academy's website. For the full text of these policies, please see _____ ~~[link].~~**[INSERT LINK]**

For user convenience, a brief summary of the key requirements of these policies follows. Please address any questions to the Academy's Information Technology Office at _____ [specify e-mail address] or call _____ [specify phone number].

All computer users are required to certify annually that (1) they have read the information security policies identified in this document, and (2) they understand and agree to abide by the information security policies applicable to them. Appropriate training will be provided to all users. **( )** In addition, all users with access to the Academy's protected health information or personally-identifiable information (e.g., social security numbers, credit/debit card information, etc.) are required to affirm that they will not store this information on mobile/portable storage devices without (1) obtaining prior authorization from the **[ ] Board [ ] School Leader (employed by the Board) [ ] Educational Service Provider**, and (2) encrypting the data.

Expectations for All Technology Users

This document summarizes the Board of Directors information security policies. Users of ~~the~~ Academy Information & Technology Resources must read these summaries, and both understand and fulfill their responsibilities under the applicable policies.

A. In many cases, operating system and application updates, along with malware protection, are all that stand between a computer and a system compromise or infection (i.e., a cybersecurity incident). The Academy Information & Technology Resources are regularly updated and provided malware protection.

[ ] Users are responsible for verifying their computers are configured to receive automated patches~~,~~ and ensuring the automated updates run so that security vulnerabilities are patched in a timely manner.

[ ] Users must also verify their malware protection is properly installed, updated, and ~~is~~ running the latest virus definitions.

[ ] Users' academy or department IT support staff is available to assist with these responsibilities.

[NOTE: END OF OPTION LANGUAGE; THE THIRD OPTION SHOULD BE SELECTED IF THE FIRST AND/OR SECOND OPTIONS ARE SELECTED.]

If Academy users access Academy Information & Technology Resources using personal communication devices (PCDs), they must verify proper security measures are active on their devices.

B. No software is 100% effective in preventing compromises or infections (i.e., cybersecurity incidents), and not all websites are safe. Users must be alert when using the Internet, especially on systems storing or processing protected and confidential data/information. One way to reduce the risk of compromise is to limit the user's nonwork~~non-work~~ related Internet activity.

C. **[DRAFTING NOTE: SELECTION OPTION #1 OR OPTION #2]**

[ ] [OPTION #1]

Unless authorized and using a device that is capable of encrypting the data/information, users are prohibited from storing Academy Confidential Data/Information on the user's computing devices.

[END OF OPTION #1]

[ ] [OPTION #2]

Because confidential data/information exists in many forms (e.g., written, spoken, electronically recorded, printed, etc.), users are responsible for properly securing this data/information at all times. This may take the form of physical security (e.g., locked cabinets, locked doors, locked building) or through digital security (e.g., passwords, multifactor authentication (MFA), biometric identification, ~~biometric authentication,~~ encryption). All users with access to the Academy's Confidential Data/Information are:

( ) prohibited from storing this data/information on any mobile computing device (e.g., laptop, tablet) or portable storage device (e.g., flash drive) that is not encrypted;

( ) required to activate their devices' available security feature(s) that prevent direct access to the data/information on the device without first verifying the identity of the user via a secure method (e.g., passcodes, MFA, biometrics, user id/password);~~.~~

This applies to both personal and Academy-provided devices when Academy Confidential Data/Information may be stored on that device (e.g., e-mail, student records, etc.). Users are prohibited from storing Academy Confidential Data/Information on any device that does not meet this basic level of security~~:~~.

( ) prohibited from storing Confidential Data/Information on any mobile /portable storage device (e.g., USB flash cards, CD-ROMs, etc.);

( ) prohibited from storing Confidential Data/Information on any mobile /portable storage device (e.g., USB flash cards, CD-ROMs, etc.) that is not encrypted;

( ) prohibited from storing Confidential Data/Information on any mobile /portable storage device (e.g., USB flash cards, CD-ROMs, etc.) that is not encrypted ~~or~~ and password-protected~~password protected~~;

( ) allowed to store Confidential Data/Information on the Academy provided cloud storage (e.g., Microsoft OneDrive). Use of other public cloud storage options for Confidential Data/Information is prohibited.

[END OF OPTION #2]

D. Academy Confidential Data/Information includes many different types of data/information, such as social security numbers, personal health information, student records, ~~and~~ bank and credit card information, and~~or~~ other personally-identifiable information.

E. Academy Confidential Data/Information must never be shared through instant messaging or peer-to-peer (P2P) file-sharing software or devices. P2P software must never be installed on machines or devices that store, process, or access confidential data/information. Academy users are required to obey copyright laws and to adhere to the applicable acceptable use and safety policies ~~acceptable use policy~~ (Policy 7540.03 (student) and Policy 7540.04 (staff)).

F. Academy Confidential Data/Information must be accessed only through one (1) of the following methods: (1) user authentication with the correct password; (2) multi-factor authentication, such as a smart card in combination with a password; or (3) biometric identification approved by the Academy's Information Technology Office. **( )** Some networked storage options supplied by the Academy are not suitable for the storage of Academy Confidential Data/Information because they do not conform to these access requirements. **( )** Likewise, third party consumer cloud computing or software-as-a-service offerings, such as Dropbox, Google Docs, iCloud, and other similar offerings, are not acceptable for the storage of Academy Confidential Data/Information unless the Academy has a current contract with these providers that includes data/information security. **[END OF OPTIONS]** If a user is not sure if a storage location is secure, the user should contact the Academy's Technology Office.

G. Machines and devices that store Academy Confidential Data/Information, or that are used to access mission critical systems (e.g., SIS, ERP, Payroll), must be used only in areas with restricted or controlled access and must be locked whenever they are left unattended. Machines and devices containing Academy Confidential Data/Information or used to access mission critical systems and resources must be set to require re-authentication after not more than _____ **(**_____**)** minutes of

inactivity. **( )** It is recognized that requiring re-authentication for teachers every _____ minutes may be disruptive to teaching. Therefore, it is the teacher's responsibility to appropriately protect Confidential Data/Information in the classroom by ensuring students, parents, volunteers, visitors, or others without authorization to view/access the data/information do not view/access it when the Confidential Data/Information is in use.

H. Academy Confidential Data/Information maintained on computers or other electronic devices should be destroyed or disposed of only in accordance with Board policy and State law. Any academy or department intending to use surplus computing devices and/or ~~and or~~ scanner/printer/copy machines or any other device that stores information must first destroy the electronic information by wiping the data from the hard drive(s), flash storage, or having this done by authorized Academy personnel and keeping the devices physically secure until transfer to Academy Surplus.

I. Users must maintain strong passwords for every Academy system and application they access that stores/processes Academy data/information. Users must change all passwords used for Academy systems in accordance with the Academy's password requirements.

J. Per the Board's e-mail policy, users must always use their official Academy-supplied e-mail address for official business. Auto-forwarding of Academy e-mail accounts is prohibited **( )**~~,~~ unless approved by the **[ ] Board [ ] School Leader ~~(employed by the Board)~~ [ ] Educational Service Provider [END OF OPTION]**. Manual forwarding of individual e-mail messages is permitted.

K. Users must immediately report lost or stolen mobile/portable devices (e.g., laptops, smartphones) or security breaches (e.g., computer viruses, hacking attempts) to the Academy's Information Technology Office and/or the Academy Security Office. If a user suspects Academy Confidential Data/Information or mission critical systems and resources are at risk, the user must make this point clear when submitting a report. Also, if a user suspects Academy Confidential Data/Information is at risk, the user should avoid taking any actions such as manually scanning the computer with antivirus software. Information Technology and/or Security employees will assess what needs to be done.

L. Users must be mindful of the risks associated with Academy Confidential Data/Information when storing, processing, or accessing data/information. If a user is not sure how to comply fully with Board policies or procedures or if the user is not sure how to conduct a process securely, the user should ask for assistance from the site or department IT support contact or the Academy's Information Technology Office. Users are expected to know their sites' information technology contact so that they can contact ~~him/her~~them when there is a need.

Expectations for Administrative Personnel

In addition to the preceding, administrative personnel must also understand and fulfill the following responsibilities. Appropriate training will be provided.

A. Each Academy site or department that is responsible for maintaining Academy Information & Technology ~~its Technology Resources and Information~~ Resources must have a designated information technology contact, plus a designated backup information technology contact. The Academy's Information Technology Office monitors the duties, responsibilities, and training of information technology contacts. Each site or department administrator that maintains their site's/department's~~its own Information & Technology Resources~~~~information technology~~ must verify that the~~its~~ IT support personnel have been trained to maintain the unit's Information & Technology Resources ~~IT resources~~ in compliance with all of the Academy's information security policies and procedures.

B. Each Academy site that stores Academy Confidential Data/Information or that operates mission critical systems must work with the Academy's Information Technology Office to perform regular vulnerability scans.

C. Each Academy site or department administrator that maintains their site's/department's ~~its own~~ Information & Technology Resources ~~information technology~~ is responsible for reporting immediately to the Academy's Information Technology Office or Security Office any time there is reason to suspect that the security of Academy Confidential Data/Information or of a mission critical system (e.g., Human Resources, Finance, Student Information Services, Payroll, e-mail, etc.) has been compromised or is at risk.

Expectations for Technology Support Personnel

In addition to all of the above, technology personnel, regardless of the site to which they are assigned, must also understand and fulfill the following responsibilities. Appropriate training will be provided.

A. IT personnel must read, understand and comply with the Board's policies and procedures that govern the use, operation and protection of IT systems and resources. The information technology security standards described in the information security policy are minimum standards required for the protection of Academy systems, including those that store/process Academy Confidential Data/Information or that are considered mission critical. Site and department IT resources for which an IT support employee is responsible must be managed in compliance with these policies and procedures. If technology personnel have questions or need assistance, it is the employee's responsibility to contact their ~~his/her~~ School Leader and/or the Academy's Information Technology Office.

( ) Technology personnel managing mission critical systems and Academy Information & Technology Resources (e.g., Human Resources, Finance, Student Information Services, Payroll, e-mail, etc.) or systems that store/process Academy Confidential Data/Information must have formal information security training. Information security training is available from the Academy's Information Technology Office. **[END OF OPTION]**

B. IT personnel are responsible for enforcing Academy password requirements for the systems and applications the IT personnel manage. System and application administrators must configure all Academy-owned and managed IT devices/systems to implement the password requirements to the degree technically feasible, in compliance with the Academy's password standards.

C. If a user is unsure how to transfer Academy Confidential Data/Information, the user should contact the site/department technology contact for assistance. If the site/department technology contact is unsure of the proper method to transfer the Confidential Data/Information, the request should be referred to the Academy's Information Technology Office.

D. IT personnel must report system and application vulnerabilities to the School Leader and/or the Academy's Information Technology Office.

E. The Academy Information Technology Office will perform regular vulnerability scans of Academy Information & Technology Resources.

F. If technology personnel suspect that the security of any data/information or of a mission critical system (e.g., Human Resources, Finance, Student Information Services, Payroll, e-mail, etc.) has been compromised or is at risk, it is their responsibility to report that immediately to the Academy's Information Technology Office and/or Security Office. No action should be taken that might inhibit investigation of an incident or make unavailable information that might assist the investigation.

G. Technology personnel are required to follow incident handling instructions as specified in the cybersecurity incident management policy and/or as directed by the Academy's Information Technology Office or Security Office in response to potentially unauthorized access of protected information.

Key Information Security Policies and Administrative Procedures

Below are brief descriptions of the Academy's policies and procedures related to information security. The full text of each policy or procedure can be found on the Academy's website or by clicking the highlighted link.

Policies

A. Policy 7540 – Technology – Authorizes the development of an Academy Information & Technology Plan to facilitate effective use of Academy Information & Technology Resources that support student learning and/or Academy business operations.

B. Policy 7540.02 – Web Accessibility, Content, Apps and Services ~~Content, Services and Apps~~ – Addresses the requirements for creation of Academy-authorized websites, web pages, and services/apps~~services and apps~~ by employees and students.

C. Policy 7540.03 – Student Technology Acceptable Use and Safety - Describes student use of Academy Information & Technology

Resources, expectations of privacy, Academy technology protection measures, areas for student training, and assigned ~~school~~ academy e-mail accounts.

D. Policy 7540.04 – Staff Technology Acceptable Use and Safety - Describes staff use of Academy Information & Technology Resources.

E. Policy 7540.05 – Academy-Issued Staff E-Mail~~E-mail~~ Account and Policy 7540.06 – Academy-Issued Student E-Mail~~E-mail~~ Account - Establishes a framework for proper use of Academy-issued~~Academy issued~~ e-mail accounts as an official business or educational tool for staff and students.

F. Policy 8305 – Information Security – The Board authorizes the **[ ] Board [ ] School Leader** ~~(employed by the Board)~~ **[ ] Educational Service Provider** to develop internal controls necessary to provide for the proper collection, classification, retention, access, and security of Academy data/information to include procedures in the event of a cybersecurity incident (e.g., an unauthorized release of information) and training for staff.

Administrative Guidelines

A. AG 8305A – Information Security Responsibilities and Policy 8305 - Information Security - Review of what every computer user, administrator, and technology support employee should know in order to ensure the security of Academy data/~~-~~information.

B. AG 7540B– Technology Director – and Policy 7540 – Technology - Describes the responsibilities for the position of Technology Director.

C. AG 7540C – Technology Governance Committee – Presents the requirements for establishing an Academy Technology Governance Committee that will create standards and procedures for proper management and protection of Academy Information & Technology Resources ~~technology resources~~.

D. AG 7540A – Staff and Student Training Regarding the Internet - Describes areas to be included in training of staff and students~~student~~ in proper use of the Internet.

E. AG 8305 – Collection, Classification, Retention, Access and Security of Academy Data/Information – Provides a framework that Academy employees can use to classify data/information for the purpose of determining the data's/information's need for protection.

F. AG 8305B - Cybersecurity~~Information Security~~ Incident Management – Presents requirements for managing and reporting information security incidents.

REVISED GUIDELINE – SPRING 2023
CYBERSECURITY ~~INFORMATION SECURITY~~ INCIDENT MANAGEMENT

This administrative guideline governs the reporting and management of security incidents involving the Academy's Information of security incidents involving the Academy's Information & Technology Resources (as defined in Bylaw 0100).

Every Board of Directors member, staff member/employee, student, parent, contractor/vendor, and visitor to ~~school~~ academy property who accesses Academy-owned or managed information through computing systems or devices ("users") must report cybersecurity ~~information security~~ incidents (as defined below) promptly per the procedures described herein.

When a cybersecurity ~~an information security~~ incident involves Academy Confidential Data/Information (as defined below) or mission critical devices (as defined below), the **[ ] School Leader ~~(employed by the Board)~~ [ ] Educational Service Provider /Technology Director/Academy's** Information Technology Office may, in coordination with the Academy's Security Office, direct the incident response and investigation. The Technology Director is authorized, in conjunction with the **[ ] School Leader ~~(employed by the Board)~~ [ ] Educational Service Provider**, to take any action necessary to mitigate the risk posed by the ~~information~~ cybersecurity incident.

An employee who puts Academy Confidential Data/Information at risk as a result of their ~~his/her~~ failure to adhere to relevant policies/administrative guidelines/the law may be subject to disciplinary consequences, up to and including termination of employment and/or referral to law enforcement. Students who fail to adhere to applicable policies/administrative guidelines/the law will be referred to ~~school~~ the Academy and/or Academy administration for review and determination of the consequences of their actions, including referral to law enforcement. Contractors and vendors who fail to adhere to applicable policies/administrative guidelines/the law may face termination of their business relationships with and/or legal action by the Academy. Parents and visitors who fail to adhere to applicable policies/administrative guidelines/the law may be denied access to Academy Information & Technology ~~Technology and Information~~ Resources and/or referral to law enforcement. Violations can in some cases also carry the risk of civil or criminal penalties.

_____ is responsible for establishing and maintaining an up-to-date cybersecurity incident ~~information security~~ management plan.

NOTE: SELECT OPTION #1 or OPTION #2

[ ] [OPTION #1]

The ~~school~~ Academy site administrator (e.g., the School Leader) or the Academy-wide department administrator, along with the Tech Specialist (or equivalent)~~[or equivalent]~~, are responsible for reporting ~~information~~ cybersecurity incidents at their site.

[END OF OPTION #1]

[ ] [OPTION #2]

The plan shall identify the primary and secondary cybersecurity incident~~information security~~ contact for each ~~school~~ Academy and Central Office/Academy-wide department (e.g., Human Resources, Treasurer/payroll, Business Services, Student/Pupil Services). Any unique requirements concerning a specific building or department must be delineated in a subsection of the plan that is particular to the given building or department.

[END OF OPTION #2]

Definitions

A. **Incident Management Plan**

The IT Department, in conjunction with Department/Division/Building Leaders, must develop and maintain a plan that contains procedures on how to handle ~~information~~ cybersecurity incidents, including contact information for site/unit personnel with the responsibility for responding to the incident, plans to contain an incident, and procedures on how to restore information.

B. **Cybersecurity~~Information Security~~ Incident**

Includes any incident that is known or has the potential to negatively impact the confidentiality, integrity, or availability of Academy information/data. This can range from the loss of a laptop, tablet or other mobile/portable storage device, ~~the~~ virus infection of an end-user workstation, or ~~a~~ breach of an Academy system by a hacker.

C. **Mission Critical Resource**

Includes any resource that is critical to the mission and operation of the Academy and any device that is running a mission critical service or stores Academy Confidential Data/Information. Mission critical services must be available. Mission critical resources for information security purposes include, for example, information/data assets, software, hardware, and facilities related to Human Resources, Finance, Student Information Services, Payroll, and e-mail~~)~~.

D. **Academy Confidential Data/Information**

Includes all data/information, in its original and duplicate form, that contains:

1. "personal identifying information", as defined by State and Federal laws;

   This includes employer tax ID numbers, ~~drivers'~~ driver's license numbers, passport numbers, SSNs, State identification card numbers, credit/debit card numbers, banking account numbers, PIN codes, digital signatures, biometric data, fingerprints, passwords,

and any other numbers or information that can be used to access a person's financial resources.

2. "protected health information" as defined by ~~the~~ HIPAA;

3. student "education records", as defined by the Family Educational Rights and Privacy Act (FERPA) and State law (R.C. 3319.321);

4. data/information that is deemed to be confidential in accordance with the Michigan Public Records Act.

( ) "card holder data"~~,~~ as defined by the Payment Card Industry (PCI) Data Security Standard (DSS).

Adherence to the procedures outlined below will streamline the handling of ~~information~~ cybersecurity incidents and minimize the timeframe during which Academy Confidential Data/Information and mission critical resources are left in a vulnerable state.

Incident Reporting

Given the risks associated with cybersecurity ~~information security~~ incidents, as well as implications for the Academy related to compliance with Federal and State regulatory requirements, it is essential that ~~school~~ academy site administrators and Academy department administrators be aware of ~~information~~ cybersecurity issues and their responsibilities for reporting and mitigating ~~information~~ cybersecurity risks.

~~School~~ Academy site administrators and Academy department administrators who manage business units that maintain and manage their site's Information & Technology Resources~~information resources~~ must designate employees as primary and back-up cybersecurity ~~information security~~ contacts, provide the Academy's Information Technology Director with the names and contact information of these individuals, update this information whenever it changes, and verify that these contacts are trained by the Academy's Technology Office to perform their duties.

Each cybersecurity ~~information security~~ contact shall serve as an intermediary between ~~his/her~~their respective Academy site or office and the Academy's Information Technology Office and must assist the site or office ~~s/he serves~~they serve in implementing cybersecurity ~~information security~~ policies and ~~information security~~ initiatives including training of site staff and in responding to ~~data breach~~ cybersecurity incidents, all in close coordination with the Academy's Information Technology Office.

Every technology user, including Board members, staff members/employees, students, parents, contractors/vendors, and visitors to campus, who has access to Board-owned or managed Information & Technology Resources ~~information resources~~ and who suspects that there may have been ~~an information~~ a cybersecurity incident (ranging from a lost or stolen laptop, tablet or other mobile/portable storage device, the virus infection of an end-user work station, or a major intrusion by a hacker) must promptly report the incident to ~~his/her~~their **[ ] School Leader ~~(employed by the Board)~~ [ ] Educational Service Provider** or director/manager and/or the ~~information security~~ cybersecurity contact for that unit/site.

The cybersecurity ~~information security~~ contact's roles and responsibilities include, but are not limited to:

A. serving as a single point of contact for the Academy's Information Technology Office regarding security efforts and ~~information~~ cybersecurity incidents that affect Academy sites;

B. aiding the Academy's Information Technology Office in improving ~~information~~ cybersecurity in the Academy by coordinating with them on security matters;

C. working with the Academy's Information Technology Office on cybersecurity incident management and response, as well as ~~assist~~ assisting the Academy's Information Technology Office, as needed, in certain activities including coordinating the following with the Academy's Technology Office:

1. ensuring proper identification and classification of mission critical devices and Academy Information & Technology Resources storing Academy Confidential Data/Information within their ~~school~~ academy site or business unit/department;

2. advising and training their site's administration, faculty, and staff on the implementation of appropriate security controls for Academy Information & Technology Resources; ~~Technology Resources (as defined in Bylaw 0100) and Information Resources;~~

3. meeting periodically with the Academy's Information Technology Office to move forward Academy security initiatives for their respective sites;

4. maintaining an up-to-date list of staff/users with access to Academy Confidential Data/Information and Controlled Data/Information in their working group and promptly notifying the Academy's Information Technology Office of any personnel changes, including transfers within the Academy;

5. providing basic security advice for all assigned systems and users within their site;

6. ensuring timely compliance with security awareness requirements, including appropriate refresher training and training of new employees;

   In consultation with the **[ ] School Leader** ~~**(employed by the Board**~~ **[ ] Educational Service Provider**, the contact will oversee the site's compliance with applicable State and Federal laws as well as Board policies regarding Academy Confidential Data/Information.

7. ensuring that any detected vulnerabilities are remediated in a timely manner;

8. advising their site regarding the implementation of appropriate security controls consistent with the Academy's cybersecurity incident management ~~information security~~ policy;

9. collecting incident response information;

The contact must provide a timely notification of the Academy's Information Technology Office regarding any ~~information~~ cyber security incidents for their respective site consistent with the cybersecurity incident management procedure. In addition, the contact must provide a timely and comprehensive response to ~~information~~ cybersecurity incidents in coordination with the Academy's Information Technology Office.

10. coordinating with the Academy's ~~information~~ cybersecurity strategic initiatives.

Each information security incident will be classified accordingly to the following "levels":

Incident Level	Examples	Investigation Type
Level 1	Violation of Board policies and administrative guidelines that relate to technology and information security.	Basic investigation of an incident.
	A virus or malware detection.	Remediation advice for an incident is provided. Device isolation, if necessary.
Level 2	Unauthorized computer/network access, misuse, or user permission issue. Computer/system theft, damage or loss. Malicious Denial of Service Attack or other attempt to interrupt normal operations.	Investigation of the incident. Notification will be provided if applicable pursuant to AG 8305C.
Level 3	Hacking or system breach to core/mission critical systems. Unauthorized release of Academy Confidential Data/Information.	Investigation of a likely or confirmed breach of a system processing/storing Academy Confidential Data/Information or a mission critical system. Investigation of information technology relevant issues performed in support of criminal or civil cases, as well as Academy internal investigations.

Notification will be provided if applicable pursuant to AG 8305C.

In the event of a possible Level 2 or 3 ~~information~~ cybersecurity incident, the user or administrator of the potentially compromised system or device should work with the site's information security contact to preserve all evidence, including leaving the possibly compromised machine powered up and online, and refraining from accessing the system or machine in any way. The information security contact will then report the incident to the Academy's Information Technology Office and/or Security Office. The Academy's Information Technology Office and the Security Office will advise how best to proceed for purposes of preserving evidence and constructing an audit trail for the investigation of the incident. As appropriate, the Academy's Security Office will coordinate with public safety and law enforcement officials.

The **[ ] School Leader** ~~**(employed by the Board)**~~ **[ ] Educational Service Provider** will coordinate all external communications with the media or the public related to any ~~information~~ cybersecurity incident.

REVISED GUIDELINE – SPRING 2023
NOTIFICATION ~~INFORMATION~~ CYBERSECURITY INCIDENT

References: R.C. 1347.12, 1349.191, 1349.192
FERPA

As required by AG 8305B, if a user, who has access to Academy Confidential Data/Information and/or to any mission critical ~~mission-critical~~ system, suspects that there may have been a cybersecurity ~~an information security~~ incident, the user must promptly report the incident to an Academy administrator who shall immediately notify the **[ ] School Leader** ~~**(employed by the Board)**~~ **[ ] Educational Service Provider** and the Academy's Information Technology Office and/or Security Office.

If a cybersecurity ~~an information security~~ incident occurs that involves the release of Academy Confidential Data/Information, the Academy will take action in accordance with State and Federal law to address the situation~~,~~ including, when appropriate and/or legally required, notifying affected individuals that their personally-identifiable information was improperly accessed and/or released. Any required notices will be provided in a timely manner.

Pursuant to State law, the Academy shall disclose any security breach of computerized personal information data ("breach of the security of the system"), following its discovery or notification of the breach of the security of the system, to any Michigan resident whose personal information (as defined below) was, or reasonably is believed to have been, accessed and acquired by an unauthorized person if the access and acquisition by the unauthorized person causes or reasonably is believed will cause a material risk of identity theft or other fraud to the resident.

For purposes of this policy, "breach of the security of the system" means unauthorized access to and acquisition of computerized data that compromises the security or confidentiality of personal information owned or licensed by the Board of ~~Education~~ Directors and that causes, reasonably is believed to have caused, or reasonably is believed will cause a material risk of identity theft or other fraud to the person or property of a~~n~~ Michigan resident.

"System" means any collection or group of related records that are kept in an organized manner, that are maintained by the Academy, and from which personal information is retrieved by the name of the individual or by some identifying number, symbol, or other identifier assigned to the individual.

"Personal information" means an individual's name, consisting of the individual's first name or first initial and last name, in combination with and linked to any one (1) or more of the following data elements, when the data elements are not encrypted, redacted, or altered by any method or technology in such a manner that the data elements are unreadable: (a) social security number; (b) driver's license number or State identification card number; or (c) account number or credit or debit card number, in combination with and linked to any required security code, access code, or password that would permit access to an individual's financial account.

The notice to individuals required by State law shall be made as expeditiously as practicable and without unreasonable delay, taking into account the time necessary to allow the Academy to determine the scope of the breach of security, to identify individuals affected by the breach, and to restore the reasonable integrity of the data system that was breached, but no later than forty-five (45) days after the discovery or notification of a breach~~,~~ unless subject to an authorized delay.

If a Federal, State, or local law enforcement agency determines that disclosure or notification to individuals required under this guideline would impede a criminal investigation~~,~~ or jeopardize homeland or national security, the notice shall be delayed until the law enforcement agency determines the disclosure or notification will not compromise the investigation or jeopardize homeland or national security.

[ ] Notice to the affected individuals is not required if, after an appropriate investigation and consultation with relevant Federal, State, or local law enforcement agencies, the Academy reasonably determines that the breach has not and will not likely result in identity theft or any other financial harm or fraud to the individuals whose personal information has been accessed. Such a determination must be documented in writing and maintained for at least _____ [e.g., five (5)] years.

The Academy will make the State-mandated disclosure or notification by one (1) of the following methods:

A. written notice

B. electronic notice, if the Academy's primary method of communication with the resident is by electronic means

C. telephone notice

The Academy may provide substitute notice in lieu of direct notice if (a) the Academy does not have sufficient contact information to provide notice in one (1) of the manners described above, (b) the cost of providing disclosure or notice would exceed $250,000, or (c) the affected class of residents exceed 500,000 persons. Such substitute notice shall include all of the following:

A. electronic mail notice if the Academy has an e-mail address for the resident

B. a conspicuous posting of the disclosure or notice on the Academy's website

C. notification to major media outlets (including print and broadcast) to the extent the cumulative total of the readership, viewing audience, or listening audience of all of the outlets so notified equal<u>s</u> seventy-five percent (75%) of the State's population

If the Academy discovers circumstances that require State-mandated disclosure pursuant to this guideline to more than 1,000 residents involved in a single occurrence of a breach of the security of the system, the Academy shall notify, without unreasonable delay, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis of the timing, distribution, and content of the disclosure given by the Academy to affected Michigan residents.

In the event of a breach of security of a system maintained by a <u>third party</u>~~third-party~~ agent, such <u>third party</u>~~third-party~~ agent shall notify the Academy of the breach of security as expeditiously as practicable, but no later than _____ [e.g., ten (10)] days following the determination of the breach of security or reason to believe the breach occurred. Upon receiving notice from a <u>third party</u>~~third-party~~ agent, the Academy shall provide the notices required above. A <u>third party</u> ~~third-party~~ agent shall provide the Academy with all information that the Academy needs to comply with its notice requirements.

An agent, pursuant to a contract entered into by the Academy prior to the date of the breach of the security of the system occurred, may provide notice as required on behalf of the Academy, so long as the contract does not conflict with any provision of R.C. 1347.12.

REVISED GUIDELINE – SPRING 2023
LITIGATION HOLD PROCEDURE

Source: F.R.C.P. 34, 37(f)
R.C.P. 34, 37(F)

Any Board member or employee who receives specific information and/or written notification regarding one (1) of the following instances shall immediately provide that information and/or written notification to the Administrator:

A. an individual, parent, or student intends to appeal a student discipline to State court;

B. litigation is imminent even though the litigation has not yet been filed in Federal or State court;

C. the Board is served with litigation~~,~~ including, but not limited to, notice of a lawsuit in Federal or State court~~,~~ or notice of a student disciplinary appeal to State court;

D. an employee, labor union, or other person intends to file a claim against the Board, its members~~member~~, employees, or agents at an administrative agency such as the Equal Employment Opportunity Commission, Michigan Civil Rights Commission, State Employment Relations Board, U.S. Department of Education Office for Civil Rights, Michigan Department of Education Office for Exceptional Children or Office of Professional Conduct, State Personnel Board of Review, or a Civil Service Commission;

E. an administrative agency, such as the Equal Employment Opportunity Commission, Michigan Civil Rights Commission, State Employment Relations Board, U.S. Department of Education Office for Civil Rights, Michigan Department of Education Office for Exceptional Children or Office of Professional Conduct, State Personnel Board of Review, or a Civil Service Commission, intends to investigate a claim filed against the Board, its members, employees, or agents;

F. a third party requests that a Board member or employee maintain information that could be at issue in litigation or potential litigation ~~against~~ involving that third party;

G. the Administrator recommends the termination of an employee to the Board pursuant to a labor contract;

H. the Board is exploring, contemplating, or initiating litigation.

Upon receipt, the Administrator shall review the specific information and/or written notification to determine whether Policy 8315 - Information Management - applies. If it does, the Administrator shall initiate a Litigation Hold applicable to all relevant information. The Administrator also will **( ) notify the Board ( ) direct the Board's legal counsel to notify the Board** ~~–~~ **[END OF OPTION]** of the scope of and reason for implementation of the Litigation Hold.

To initiate a "Litigation Hold," the Administrator or designee shall immediately notify the AcademySchool Records Commission to suspend all records disposal procedures until the matter under the "Litigation Hold" is fully defined and information falling under the "Litigation Hold" is identified. The notification to the AcademySchool Records Commission shall be documented.

A "Litigation Hold" is a procedure that identifies and preserves information relevant to a matter by identifying individuals in possession or custody of paper documents, electronically stored information ("ESI"), and electronic media storing ESI, and informing them of their obligation to preserve such information outside the "Records Retention Schedule". Third parties with control or custody of paper documents, ESI, or electronic media storing ESI also are notified of the "Litigation Hold" and requested to preserve that information until notified otherwise. All information covered by a "Litigation Hold" must be prospectively preserved and cannot be disposed of under the "Records Retention and Disposal" requirements until the "Litigation Hold" is removed.

Definitions

"Information" includes all paper documents and ESI.

"Documents" includes, but is not limited to, writings, drawings, graphs, charts, photographs, blueprints, sound/audio recordings, images, video recordings, images and other data or data compilations stored in any medium from which information can be obtained or translated if necessary.

"ESI" means any type of information that is created, used, and stored in digital form and accessible by digital means. It includes all data, digital documents or files, or other information contained on any media type (e.g., tape, hard disk drive, cloud storage, or some yet-to-be-created storage technology). Specifically, it includes, but is not limited to, writings, drawings, graphs, charts, photographs, blueprints, sound recordings, images, video recordings, and other data or data compilations stored in any electronic media from which information can be obtained or translated if necessary. Examples include: e-mails and their attachments, text and instant messages, communications conducted in ephemeral messaging applications or in workplace collaboration tools, word processing documents, spreadsheets, digital photographs/pictures, videos, application program and data files, data/information stored in databases, data files, metadata, system files, electronic calendar appointments, scheduling program files, digital scans (including ~~It includes, but is not limited to, e-mails, e-mail attachments, instant messages, word processing files, spreadsheets, pictures, application program and data files, databases, data files, metadata, system files, electronic calendar appointments, scheduling program files,~~ TIFF files, PDF files, MPG files, JPG files, and GIF files, network share files, internal websites, external websites, newsgroups, directories, security and access information, legacy data, audio recordings, voice mails, phone/call logs, faxes, internet/browser histories, caches, cookies, and/or logs of activity on computer systems (whether internal to the Academy of external) that may have been used to process or store electronic data). ESI also includes data/information from cloud applications (e.g., educational or operational apps/services), electronic records of online activity (e.g., social media postings), and data generated or stored by devices connected to the Internet of Things (IoT).

"Electronic Media" includes, but is not limited to, computer hard drives (including portable hard disk drives "HDD's"), floppy drives, disaster recovery media, and storage media (including DVD's CD's, floppy discs, Zip discs/drives, Jazz discs/drives, USB memory drives,

jump discs/drives, flash discs/drives, keychain discs/drives, thumb discs/drives, smart cards, microfilm~~micro-film~~, backup tapes, cassette tapes, cartridges, etc.)~~,~~ accessed, used, and/or stored on/in/through the following locations: networks and servers, whether internal or external (including the cloud); laptop and desktop work computers; home and personal computers; other computer systems; databases; backup computers or servers, whether internal or external (including cloud storage); archives; mobile devices (e.g., mobile/cellular phones and tablet computers, personal digital assistants ("PDAs" – including Palm, Blackberry, ~~cellular phone, tablet PC,~~ etc.); pagers; firewalls; audit trails and logs, printers; copiers; scanners; digital cameras; photographic devices; or video cameras and devices. Electronic media also includes social media sites (e.g., Facebook, Twitter, LinkedIn) and ~~shall also include~~ any item containing or maintaining ESI that is obtained by the Academy~~School~~ for Board member or employee usage or that a Board member or employee uses for such purpose (even if privately owned by the Board member or employee) from the date this policy was first ~~is~~ adopted into the future.

ESI Team

The Administrator **( ) may ( ) will [END OF OPTION]** utilize an Electronically Stored Information Team ("ESI Team") to implement a "Litigation Hold". The ESI Team shall be responsible for recommending to the Administrator actions necessary to implement the "Litigation Hold" and for any other action(s) delegated~~designated~~ to the ESI Team ~~it~~ by the Administrator. The ESI Team shall be comprised of the ~~School~~ Academy ~~Record~~ Records Custodian, the primary Academy~~School~~ Information Technology administrator, an Academy ~~School~~ Operations ~~Administrator~~administrator, and any other individual the Administrator ~~designates~~assigns. If the Academy ~~School~~ is utilizing an attorney to handle the matter that is the cause of the "Litigation Hold," the attorney will also be a member of the ESI Team or attend key ESI Team meetings as directed by the Administrator. The ESI Team shall document any meetings held and any recommended actions.

CHOOSE EITHER OPTION #1 OR OPTION #2

OPTION #1

Choose Option #1 if the Board elected "the Administrator MAY utilize an ESI Team"

[ ] The Administrator ~~or designee~~, or the ESI Team (if the Administrator determines to utilize one), will (a) define the matter under the "Litigation Hold"; (b) identify information falling under the "Litigation Hold"; (c) identify all individuals and third party entities who have custody of documents, ESI, or electronic media containing ESI regarding the matter under the "Litigation Hold"; and (d) identify all individuals responsible for records disposal "Records Retention and Disposal". ~~If~~ After the ESI Team completed the above actions, it will report the above information to the Administrator. The Administrator ~~or designee~~ will notify all identified individuals, third party entities, and the Academy~~School~~ Records Commission of the "Litigation Hold" and their responsibility to preserve all information regarding the "Litigation Hold" matter in their custody or control in a readily accessible form. After distribution of the "Litigation Hold" notifications, the ESI Team (if one is used) or the Administrator ~~or designee~~ shall be responsible for regularly verifying that all documents, ESI, and electronic media containing ESI regarding the "Litigation Hold" matter are properly preserved. The ESI Team (if one is used) or the Administrator ~~or designee~~ will review the "Litigation Hold" as necessary, and at least on a **( ) quarterly ( ) semi-annual ( ) annual [END OF OPTIONS]** basis, the Administrator ~~or designee~~ will reissue the Litigation Hold notice to the affected

individuals and third party entities to remind them of their ongoing duty to properly preserve all information covered by the "Litigation Hold". The Administrator ~~or designee~~, in conjunction with the ESI Team (if one is used), will document all steps taken to implement the "Litigation Hold".

[END OF OPTION #1]

OPTION #2

Choose Option #2 if the Board chose "the Administrator WILL utilize an ESI Team"

~~[ ]~~ The ESI Team will (a) define the matter under the "Litigation Hold"; (b) identify information falling under the "Litigation Hold"; (c) identify all individuals and third party entities who have custody of documents, ESI, or electronic media containing ESI regarding the matter under the "Litigation Hold"; and (d) identify all individuals responsible for records disposal under "Records Retention and Disposal". The ESI Team will report the above information to the Administrator. The Administrator ~~or designee~~ will notify all identified individuals, third party entities, and the Academy~~School~~ Records Commission of the "Litigation Hold" and their responsibility to preserve all information regarding the "Litigation Hold" matter in their custody or control in a readily accessible form. After distribution of the "Litigation Hold" notifications, the ESI Team shall be responsible for regularly verifying that all documents, ESI, and electronic media containing ESI regarding the "Litigation Hold" matter are properly preserved. The ESI Team will review the "Litigation Hold" as necessary, and at least on a **( ) quarterly ( ) semi-annual ( ) annual [END OF OPTIONS]** basis, the Administrator ~~or designee~~ will reissue the "Litigation Hold" notice to affected individuals and third party entities to remind them of their ongoing duty to properly preserve all information covered by the "Litigation Hold". The ESI Team, in conjunction with the Administrator ~~or designee~~, will document all steps taken to implement the "Litigation Hold".

[END OF OPTION #2]

A "Litigation Hold" shall remain in place until removed by the **( ) School Leader ( ) Educational Service Provider ( )** Board. A "Litigation Hold" may be removed when the litigation or administrative agency matter has been resolved or can no longer be initiated. The Administrator ~~or designee~~ shall notify the Academy~~School~~ Records Commission and all individuals and third party entities notified of a "Litigation Hold" when the “Litigation Hold" for a matter is removed.

This administrative guideline, along with Policy 8315, shall be posted and distributed in a manner that places all Board members and employees on notice of their responsibilities under Policy 8315 - "Information Management" – and this administrative guideline.

Records Retention and Disposal Schedule for – Michigan Public Schools (Education Bulletin #522 Revised)