THE ASSOCIATION FOR MENTALLY ILL CHILDREN OF WESTCHESTER, INC.

THE CLEAR VIEW SCHOOL

CHILDREN'S INTERNET PROTECTION ACT (CIPA) POLICY

Use of the Internet in the School Setting

It is the policy of The Clear View School to encourage the use of the Internet in the School setting for educational purposes. Internet programs are used to teach and practice skills, to gain information, to learn research methods and to develop critical thinking. Students have access to the Internet on laptops, chrome books, desktops and iPads. During the school day students use only Clear View computing devices; students may not use personally-owned technology on school premises.

Filtering

The School has installed Internet filtering software to block student access to inappropriate and/or harmful web-site content. The software works by scanning website addresses and web site content for objectionable words and concepts. When the software finds any such objectionable words or concepts it denies the user access to them. At present the School is utilizing Dell's Sonic Wall content filter with screening categories that are industry standard. Additional sites are added and some restrictions may be deleted for specific study purposes by the School's IT consultant working in collaboration with classroom teachers.

Safety and Security

Clear View students do not have access to e-mail, social media or chat rooms on School computers or during the school day on personal devices. Social media and chat rooms are blocked for both students and teachers by the fire wall currently in place. All use of the internet is supervised.

In addition, the School monitors student online activities and any inappropriate usage will be dealt with promptly and appropriately, on an individualized basis, by teachers or therapists.

Unauthorized Access

The School takes all steps necessary to minimize the risk of unauthorized disclosure of student record information or other personal information about students. All electronic systems containing student record information require passwords for access, and the School has established a system of permissions that limit access of information to authorized users who have a legitimate educational interest in obtaining access to information. Student accounts do not have access to educational record data.

Students may not download, add or install new programs, software or hardware onto school-owned computers.

Unauthorized access by Students ("hacking") will result in measures that are consistent with the School's disciplinary code and procedures for behavioral intervention and guidance.

Unauthorized Disclosure, Use, and Dissemination of Personal Information regarding Students

Safeguards associated with industry standards and best practices, including encryption, firewalls and password protections are in place to protect student data which is or may be stored or transferred electronically.

Any data stored or maintained electronically will be made available to parents or guardians on request, in accordance with the Family Education Rights and Privacy Act (FERPA). Such records will be released to third parties only with parental consent or as authorized by FERPA. A parent or guardian may be asked for information or verifications necessary to ensure that he or she is in fact the student's parent or guardian and authorized to receive individually identifiable information. Data may be released to third parties acting as school officials as defined by FERPA, but only if release of such data is directly related to a service being provided to the School and the school officials have legitimate educational interests.

Personally identifiable information maintained by the School will not be sold or released for any commercial or marketing purposes.

Revised: 12/8/2017