

# Computer and Information Network

## Acceptable Use Policy

### Horizon Christian Elementary School

#### Purpose

The internet is an essential element in 21<sup>st</sup> century life and will only continue to grow in importance and pervasiveness. Considering such, the school has a duty to provide students with high quality internet access as part of their learning experience. The internet benefits education by providing access to world-wide educational resources including museums, art galleries, access to experts in various fields, and a vast amount of reference material. The purpose is to advance and promote educational opportunities, innovation and educational excellence; equipping our students for the technology world of tomorrow.

#### Privacy and Administrator Access

Occasionally students might be able to access their personal email through school computers. Students must immediately tell a teacher if they receive offensive email. Students must not reveal personal information about themselves or others in email, IM, or other forms which would include address, phone number, age, school or grade; and absolutely must not arrange to meet anyone met online. The forwarding of chain letters is not permitted. The school reserves the right to inspect a student's email for monitoring purposes.

All storage areas in the HCES network including local hard drives and student files on the server are school property and subject to inspection the same as student lockers. Internet messages (email, IM, and chat rooms) are public communication and are *not* private. HCES staff may review communication to maintain integrity system-wide and ensure that students are using the system in a responsible manner. **Users should not assume that uses of the HCES network are private.**

#### Student Access

Grades 1-6 will gain access to the internet after they take part in a discussion of this policy in technology class and a signed AUP agreement by a parent or guardian is on file. All student use of the internet will be done under faculty supervision. Lower elementary grades (1-3) will have access to the internet after adult demonstration and will be directed to specific, approved on-line material. Parents will be asked to sign and return a consent form. Upper elementary grades (4-6) will have greater access to the internet for research purposes. Students will be directed to specific material and allowed to follow related links under adult supervision. Should the curriculum require real-time communication online students shall only use regulated educational chat rooms and only when they directly fit into the educational goals. This use will be supervised and the importance of chat room safety emphasized. If instant messaging is allowed during school, it will be limited to other schoolmates.

## **The Internet**

Students will be taught what internet use is acceptable and what is not, and be given clear objectives for internet use. Staff will guide students in on-line activities that will support appropriate learning objectives for the student's age and maturity. Students will be educated in the effective use of the internet in research, retrieval, and evaluation. Ideally, inappropriate material would not be visible to students, but this is not easy to achieve and cannot be guaranteed. Unfortunately students may come across inappropriate material, despite all attempts at filtering. Students shall be taught how to validate information before accepting accuracy, acknowledge the source of information used and respect copyright laws.

## **User Responsibility**

Rules for computer/internet use will be posted in all rooms where computers are used. Students will be instructed in proper computer/internet use at the start of the school year and again halfway through the year. Instruction in safe and responsible use shall be reviewed periodically throughout the school year.

- Students are expected to follow common network etiquette, also called 'netiquette,' as well as school behavior guidelines. Students are expected to be polite, kind, and respectful - avoiding any sarcasm and slang that without face to face context may be hurtful or otherwise misinterpreted. Additionally they may not use any language that is considered offensive or threatening to persons of a particular race, gender, religion, or with disabilities; and any language that is offensive or insulting to the other gender.
- Students are responsible for making back-up copies of their documents that are critical to their use.
- Students are responsible for immediately notifying the technology department of any possible security problems or of damage to the computer they are assigned.
- HCES assumes no responsibility for unauthorized charges, costs, or illegal uses.
- Staff members are not expected to monitor student's use at every moment. Each student will take individual responsibility for his or her appropriate use of the internet.

## **Personal Safety**

Internet filtering is provided by Sterling. In addition the school maintains a blocked site list and has enabled rating filtering within Internet Explorer which is set at the lowest allowable. Students are instructed to go only to websites in the favorites list and are able to request websites for review to be added. Due to the rapidly changing nature of the internet we cannot guarantee blocking of all objectionable material and thus we will not to accept liability if a student inadvertently or purposefully accesses objectionable material.

## **Unacceptable Uses**

At no time is it acceptable for a student to:

- Make public private or personal information about self or another person.
- Attempt to access system files, security files, or another student's files.
- Access or distribute objectionable material.
- Use school computers in any way that contributes or involves illegal activity.
- Commit plagiarism; taking material from another and presenting it as their own.
- Violate copyright laws.

## **Behaviors and Consequences**

Inappropriate conduct on the HCES network will be subject to disciplinary action. Consequences may range from a warning and reduction of daily points to being denied school computer access for a set time. Repeated problem behavior will be dealt with in accordance with HCES disciplinary policy.

- Tampering with HCES computer security systems, applications, documents, or equipment will be considered vandalism, destruction, and defacement of school property.

*Please be advised, it is a federal offense (Felony) to break into any security systems. Financial and legal consequences of such actions are the responsibility of the user and student's parent or guardian.*

- Vandalism will result in cancellation of privileges, disciplinary action and restitution for costs associated with hardware, software, and system restoration. Vandalism is defined as any malicious attempt to harm or destroy data of another user, the internet, hardware, or network software. This includes, but is not limited to, the uploading or creating of computer viruses.

## **School Website**

The school website will not publish staff or student personal information. Student full names will not be used anywhere on the website, especially in association with photographs. Written permission from a parent or guardian will be obtained before photographs of student are posted on the school website. We strive to comply with all COPPA and CIPA laws.

---

HCES reserves the right to revise this policy at any time. The most current copy may be found on Edline, on the school website and at the school office. Thank you to the Bellingham School District for allowing parts of their Acceptable Use Policy in creating our policy and Kent County Council for their tools and assistance.

---