

**CHARLESTON COMMUNITY UNIT DISTRICT NO. 1
STUDENT REGISTRATION INFORMATION**

Student Name: _____

Last First Middle

Grade Male Female

Address: _____

City State Zip

Date of Birth: _____

Country of Birth USA Other (please specify)

Are you a resident of Charleston School District?
 Yes No

Please list other siblings in the household.

| <u>Sibling Name</u> | <u>Sibling Birthdate</u> |
|---------------------|--------------------------|
| _____ | _____ |
| _____ | _____ |
| _____ | _____ |
| _____ | _____ |

Student lives with (Please check one)

Father and Mother Mother only

Father only Foster Parents

Other (specify) _____

Guardian 1: _____

Address: _____

City, State, Zip: _____

Primary Phone: _____

Work Phone: _____

Cell Phone #: _____

E-mail address: _____

Guardian 2: _____

Address: _____

City, State, Zip: _____

Primary Phone: _____

Work Phone: _____

Cell Phone #: _____

E-mail address: _____

See Reverse Side to Complete Race and Ethnicity Information.

All students are provided equal opportunities in all education programs for all services. No person shall be discriminated against on the basis of race, color, creed, national origin, gender, sexual orientation, age, ancestry, marital status, citizenship status, or mental or physical disability in any of its programs, activities, services or benefits. All students are guaranteed equal access to Educational and extra-curricular activities as required by Illinois PA 79-597 and Title IX of the 1973 Educational Amendments..

By signing this form, I agree that the above information is correct.

Signature of Parent/Guardian: _____ Date: _____

RACE AND ETHNICITY DATA COLLECTION

INSTRUCTIONS: This form is to be filled out by the student’s parents or guardians, and both questions must be answered. Part A asks about the student’s ethnicity and Part B asks about the student’s race. If you decline to respond to either question, the school district is required to provide the missing information by observer identification.

PART A: Is this student Hispanic/Latino? (A person of Cuban, Mexican, Puerto Rican, South or Central American, or other Spanish culture or origin, regardless of race.)

Choose only one.

No, not Hispanic/Latino

Yes, Hispanic/Latino

PART B: What is the student’s race? Choose one or more

American Indian or Alaska Native (A person having origins in any of the original peoples of North and South America, including Central America, and who maintains tribal affiliation or community attachment.)

Asian (A person having origins in any of the original peoples of the Far East, Southeast Asia, or the Indian subcontinent including, for example, Cambodia, China, India, Japan, Korea, Malaysia, Pakistan, the Philippine Islands, Thailand, and Vietnam.)

Black or African American (A person having origins in any of the black racial groups of Africa.)

Native Hawaiian or Other Pacific Islander (A person having origins in any of the original peoples of Hawaii, Guam, Samoa, or other Pacific Islands.)

White (A person having origins in any of the original peoples of Europe, the Middle East, or North Africa.)

HOME LANGUAGE SURVEY

Section 228.15: Identification

1. Is a language other than English spoken in the home, and, if so, which language?

2. Does the student speak a language other than English, and, if so, which language?

Student’s Name

School

Grade

Parent/Guardian Printed Name

Parent/Guardian Signature

(To be placed in student’s temporary file)



CHARLESTON

C U S D N U M B E R O N E

Jefferson Elementary School • www.charleston.k12.il.us

Phone: (217) 639-7000 801 Jefferson Avenue, Charleston, IL 61920 Fax: (217) 639-7005

REQUEST FOR TRANSFER OF RECORDS

_____ has requested that your school district send their
(Parent)
student(s) records to: Please send all permanent and temporary record data, including IEP for this student(s).

Jefferson Elementary School
ATTN: Student Records Secretary
801 Jefferson Avenue
Charleston, IL 61920
PH. (217) 639-7000 FAX (217) 639-7005
metzgerl@charleston.k12.il.us

Additionally: Please include physical/dental exams and health records. Thank you.

Sincerely,

Todd J. Vilardo, Ed.D.

Todd J. Vilardo, Ed.D.
Superintendent of Schools

Student(s) Name _____ Grade Level _____

_____ Grade Level _____

Parent/Guardian _____

School Last Attended _____

(Address)

(City) (State) (Zip) Phone # Fax #

I authorize the release of information for the above named student(s) to be sent to the identified individual or agency above.

Date _____

Signature _____

Instruction

Administrative Procedure - Acceptable Use of the District's Electronic Networks

All use of the District's *electronic networks* shall be consistent with the District's goal of promoting educational excellence by facilitating resource sharing, innovation, and communication. These procedures do not attempt to state all required or prohibited behavior by users. However, some specific examples are provided. **The failure of any user to follow these procedures will result in the loss of privileges, disciplinary action, and/or legal action.**

Terms and Conditions

The term *electronic networks* includes all of the District's technology resources, including, but not limited to:

1. The District's local-area and wide-area networks, including wireless networks (Wi-Fi), District-provided Wi-Fi hotspots, and any District servers or other networking infrastructure;
2. Access to the Internet or other online resources via the District's networking infrastructure or to any District-issued online account from any computer or device, regardless of location;
3. District-owned and District-issued computers, laptops, tablets, phones, or similar devices.

Acceptable Use - Access to the District's electronic networks must be: (a) for the purpose of education or research, and be consistent with the District's educational objectives, or (b) for legitimate business use.

Privileges - Use of the District's electronic networks is a privilege, not a right, and inappropriate use may result in a cancellation of those privileges, disciplinary action, and/or appropriate legal action. The system administrator or Building Principal will make all decisions regarding whether or not a user has violated these procedures and may deny, revoke, or suspend access at any time. His or her decision is final.

Unacceptable Use - The user is responsible for his or her actions and activities involving the electronic networks. Some examples of unacceptable uses are:

- a. Using the electronic networks for any illegal activity, including violation of copyright or other intellectual property rights or contracts, or transmitting any material in violation of any State or federal law;
- b. Using the electronic networks to engage in conduct prohibited by board policy;
- c. Unauthorized downloading of software or other files, regardless of whether it is copyrighted or scanned for malware;
- d. Unauthorized use of personal removable media devices (such as flash or thumb drives);
- e. Downloading of copyrighted material for other than personal use;
- f. Using the electronic networks for private financial or commercial gain;

- g. Wastefully using resources, such as file space;
- h. Hacking or attempting to hack or gain unauthorized access to files, accounts, resources, or entities by any means;
- i. Invading the privacy of individuals, including the unauthorized disclosure, dissemination, and use of information about anyone that is of a personal nature, such as a photograph or video;
- j. Using another user's account or password;
- k. Disclosing any network or account password (including your own) to any other person, unless requested by the system administrator;
- l. Posting or sending material authored or created by another without his/her consent;
- m. Posting or sending anonymous messages;
- n. Creating or forwarding chain letters, spam, or other unsolicited messages;
- o. Using the electronic networks for commercial or private advertising;
- p. Accessing, sending, posting, publishing, or displaying any abusive, obscene, profane, sexual, threatening, harassing, illegal, or knowingly false material;
- q. Misrepresenting the user's identity or the identity of others; and
- r. Using the electronic networks while access privileges are suspended or revoked.

Network Etiquette - The user is expected to abide by the generally accepted rules of network etiquette. These include, but are not limited to, the following:

- a. Be polite. Do not become abusive in messages to others.
- b. Use appropriate language. Do not swear, or use vulgarities or any other inappropriate language.
- c. Do not reveal personal information, including the addresses or telephone numbers, of students or colleagues.
- d. Recognize that the District's electronic networks are not private. People who operate District technology have access to all email and other data. Messages or other evidence relating to or in support of illegal activities may be reported to the authorities.
- e. Do not use the networks in any way that would disrupt its use by other users.
- f. Consider all communications and information accessible via the electronic networks to be private property.

No Warranties - The District makes no warranties of any kind, whether expressed or implied, for the service it is providing. The District will not be responsible for any damages the user suffers. This includes loss of data resulting from delays, non-deliveries, missed-deliveries, or service interruptions caused by its negligence or the user's errors or omissions. Use of any information obtained via the

Internet is at the user's own risk. The District specifically denies any responsibility for the accuracy or quality of information obtained through its services.

Indemnification - By using the District's electronic networks, the user agrees to indemnify the District for any losses, costs, or damages, including reasonable attorney fees, incurred by the District relating to, or arising out of, any violation of these procedures.

Security - Network security is a high priority. If the user can identify or suspects a security problem on the network, the user must promptly notify the system administrator or Building Principal. Do not demonstrate the problem to other users. Keep user account(s) and password(s) confidential. Do not use another individual's account without written permission from that individual. Attempts to log-on to the network as a system administrator will result in cancellation of user privileges. Any user identified as a security risk may be denied access to the networks.

Vandalism - Vandalism will result in cancellation of privileges and other disciplinary action. Vandalism is defined as any malicious attempt to harm or destroy data of another user, the Internet, or any other network. This includes, but is not limited to, the uploading or creation of malware, such as viruses and spyware.

Telephone Charges - The District assumes no responsibility for any unauthorized charges or fees, including telephone charges, texting or data use charges, long-distance charges, per-minute surcharges, and/or equipment or line costs.

Copyright Web Publishing Rules - Copyright law and District policy prohibit the re-publishing of text or graphics found on the Internet or on District websites or file servers/cloud storage without explicit written permission.

- a. For each re-publication (on a website or file server) of a graphic or a text file that was produced externally, there must be a notice at the bottom of the page crediting the original producer and noting how and when permission was granted. If possible, the notice should also include the web address of the original source.
- b. Students and staff engaged in producing web pages must provide Director of Education Technology with email or hard copy permissions before the web pages are published. Printed evidence of the status of *public domain* documents must be provided.
- c. The absence of a copyright notice may not be interpreted as permission to copy the materials. Only the copyright owner may provide the permission. The manager of the website displaying the material may not be considered a source of permission.
- d. The *fair use* rules governing student reports in classrooms are less stringent and permit limited use of graphics and text.
- e. Student work may only be published if there is written permission from both the parent/guardian and student.

Use of Email - The District's email system, and its constituent software, hardware, and data files, are owned and controlled by the District. The District provides email to aid students and staff members in fulfilling their duties and responsibilities, and as an education tool.

- a. The District reserves the right to access and disclose the contents of any account on its system, without prior notice or permission from the account's user. Unauthorized access by any student or staff member to an email account is strictly prohibited.

- b. Each person should use the same degree of care in drafting an email message as would be put into a written memorandum or document. Nothing should be transmitted in an email message that would be inappropriate in a letter or memorandum.
- c. Electronic messages transmitted via the District's Internet gateway carry with them an identification of the user's Internet *domain*. This domain is a registered name and identifies the author as being with the District. Great care should be taken, therefore, in the composition of such messages and how such messages might reflect on the name and reputation of the District. Users will be held personally responsible for the content of any and all email messages transmitted to external recipients.
- d. Any message received from an unknown sender via the Internet, such as spam or potential phishing emails, should either be immediately deleted or forwarded to the system administrator. Downloading any file attached to any Internet-based message is prohibited unless the user is certain of that message's authenticity and the nature of the file so transmitted.
- e. Use of the District's email system constitutes consent to these regulations.

Internet Safety

Internet access is limited to only those *acceptable uses* as detailed in these procedures. Internet safety is supported if users will not engage in *unacceptable uses*, as detailed in these procedures, and otherwise follow these procedures.

Staff members shall supervise students while students are using District Internet access to ensure that the students abide by the *Terms and Conditions* for Internet access contained in these procedures.

Each District computer with Internet access has a filtering device that blocks entry to visual depictions that are: (1) obscene, (2) pornographic, or (3) harmful or inappropriate for students, as defined by the Children's Internet Protection Act and as determined by the Superintendent or designee.

The system administrator and Building Principals shall monitor student Internet access.

LEGAL REF.: 20 U.S.C. §7131, Elementary and Secondary Education Act.
 47 U.S.C. §254(h) and (l), Children's Internet Protection Act.
 720 ILCS 135/, Harassing and Obscene Communications Act.

ADOPTED: July 19, 2017
Revised: September 14, 2021

Charleston Community Unit School District #1
Student Authorization on the Acceptable Use Procedure
for Information and Communication Technologies Access

This form accompanies Administrative Procedure 6:235-AP1, *Acceptable Use Procedure for Information and Communication Technologies*. Every student, and if the student is a minor their parent/guardian, must sign this Authorization as a condition for student's use of the District's information and communication technologies. The signature(s) at the end of this document is legally binding and indicates that the individual(s) has read the terms and conditions carefully and understands their significance.

I understand and will abide by the *Acceptable Use Procedure for Information and Communication Technologies*. I understand that the District and/or its agents may access and monitor my accounts, my files and my utilization on ICT resources without prior notice to me. I further understand that should I commit any violation, school disciplinary action, limitation or loss of my access privileges and/or appropriate legal action may be taken. I waive any right to privacy when using district ICT resources including information created, received, transmitted and stored on these resources. In consideration for using the District's ICT resources and having access to public networks, I hereby release the School District and its Board members, employees, and agents from any claims and damages arising from my use of, or inability to use the Internet.

DATE: _____

 STUDENT'S SIGNATURE

 STUDENT'S NAME (*Please Print*):

 GRADE LEVEL

I have read the *Acceptable Use Procedure for Information and Communication Technologies* and discussed it with my child. I understand that access is designed for educational purposes and that the District has taken precautions to restrict inappropriate materials. However, I also recognize it is impossible for the District to filter access to all inappropriate materials. I will hold harmless the District, its employees, agents, or Board members, for any harm caused by materials or software obtained via the ICT resources. I accept full responsibility for supervision if and when my child's use is not in a school setting.

DATE: _____

 PARENT/GUARDIAN SIGNATURE:

 PARENT/GUARDIAN NAME (*Please Print*):

Adopted: June 20, 2012