

# Orange County Public Schools

## Technology Use Guidelines

### 2025-2026

#### General Statement

All use of the Orange County School Division's computer system shall be consistent with the School Board's goal of promoting educational excellence by facilitating resource sharing, innovation, and communication.

#### Definitions

The term "**computer system**" includes, but is not limited to, hardware, software, data, communication lines and devices, terminals, display devices, printers, CD, DVD and other media devices, tape or flash drives, storage devices, servers, and personal computers, tablets, laptops, telephones, cameras, projectors, multimedia devices, workstations, the internet and any other electronic services and any other internal or external network. This includes any devices that may be connected to or used to connect to the school division's network or electronically stored division material.

#### Computer System Use-Terms and Conditions

1. **Acceptable Use.** Access to the Division's computer system shall be (1) for the purposes of education or research and be consistent with the educational objectives of the Division or (2) for legitimate school business.
2. **Privilege.** The use of the Division's computer system is a privilege, not a right. While removal of access to computer systems may hinder a student's educational opportunities, in some cases it may be required.
3. **Unacceptable Use.** Each user is responsible for their actions on the computer system. Prohibited conduct includes but is not limited to:
  - accessing the network using another user's credentials or allowing someone to access the network using the credentials of someone else.
  - attempting to gain access to the network by spoofing or otherwise impersonating another user or client device.
  - using the network for any illegal or unauthorized activity, including violation of copyright or contracts, or transmitting any material in violation of any federal, state, or local law.
  - sending, receiving, viewing or downloading illegal material via the computer system.

- unauthorized downloading of software. using the computer system for private, financial or commercial purposes.
- wastefully using resources, such as file space.
- gaining unauthorized access to resources or entities.
- using tactics, software, or websites to attempt to bypass security/filtering.
- posting material created by another without their consent.
- submitting, posting, publishing, or displaying any obscene, profane, threatening, illegal, or other inappropriate material.
- Disclosing, use, dissemination or any other form of spreading or sharing photographs or any other personal information relating to or regarding minors
- using the computer system while access privileges are suspended or revoked.
- vandalizing the computer system, including destroying data by creating or spreading viruses or by other means.
- intimidating, harassing, bullying, or coercing others. threatening illegal or immoral acts.

**4. Network Etiquette.** Each user is expected to abide by generally accepted rules of etiquette, including the following:

- be polite.
- users shall not forge, intercept or interfere with electronic mail messages.
- use of obscene, lewd, profane, lascivious, threatening, or disrespectful language is prohibited.
- users shall not post personal information other than directory information as defined in Policy JO: Student Records about themselves or others.
- users shall respect the computer system's resource limits.
- users shall not use the computer system to disrupt others.
- users shall not modify or delete data owned by others.

**5. Liability.** The School Board makes no warranties for the computer system it provides. The School Board shall not be responsible for any damages to the user from use of the computer system, including loss of data, non-delivery or missed delivery of information, or service interruptions. OCPS is not responsible for the accuracy or quality of information obtained through the computer system. The user agrees to indemnify the School Board for any losses, costs, or damages incurred by the School Board relating to or arising out of any violation of these procedures.

**6. Security.** Computer system security is a high priority for the school division. If any user identifies a security problem, the user shall notify the building principal or system administrator immediately. All users shall keep their passwords confidential and shall follow computer virus protection procedures. Users shall not download sensitive student or staff data onto a mobile device. Users shall be required to lock their computers when away from their device.

**7. Vandalism.** Intentional destruction of or interference with any part of the computer system through creating or downloading malicious computer software, including viruses, or by any other means is prohibited.

**8. Charges.** The School Division assumes no responsibility for any unauthorized charges or fees as a result of using the computer system, including telephone, data, or long-distance charges.

9. **Email.** The School Division's email system is controlled by the School Division. The School Division may provide email to aid students and staff in fulfilling their duties and as an education tool. Email is not private. Students' email will be monitored. The email of staff may be monitored and accessed by the School Division. All email shall be archived in accordance with requirements set forth by the Library of Virginia. Unauthorized access to an email account by any student or employee is prohibited. Users may be held responsible and personally liable for the content of any email message they create or that is created under their account or password. Downloading any file attached to an email message is prohibited unless the user is reasonably certain of that message's authenticity and the nature of the file. Any uncertainty in email communication or email files should be reported to [spam-alerts@ocss-va.org](mailto:spam-alerts@ocss-va.org). Staff members must be cautious when sending any student or staff information that may be considered confidential and/or legally privileged (see FERPA).

10. **Enforcement.** Software can and may be installed on the division's computers that have or may have access to the internet so as to block pornography, gambling, obscenity and other resources as necessary. OCPS seeks to comply with C.O.P.P.A. and C.I.P.A. laws and filters, to the best of its ability, objectionable content but does not claim for any filter to be 100% accurate. The online activities of users may also be monitored manually. Any violation of these regulations shall result in loss of computer system privileges and may also result in appropriate disciplinary action, as determined by School Board policy, or legal action.