

Ipswich Public Schools Staff Computer Use Agreement

In compliance with Ipswich Public Schools (IPS) Policies IJND, IJNDB, IJNDD and federal law, the purpose of this agreement is to inform employees of the district's procedures related to staff internet and electronic media use. IPS has taken measures to protect students from obscene information and restrict access to materials that are harmful to minors. Any action taken that may expose IPS to risks of unauthorized access to data, disclosure of information, legal liability, potential system failure, or compromised user safety is prohibited. Failure to follow all or part of these guidelines may result in disciplinary action up to and including termination of employment and/or criminal prosecution. IPS has implemented methods to ensure approved online service providers can access only student records in which they have a legitimate educational interest. The service providers are under the direct control of the district with regard to the use and maintenance of the records, and the provider must adhere to all government enforced regulations regarding use and access of district information. Disclosure to other parties without authorization is prohibited.

Email

The IPS email system has been provided to facilitate internal and external communication for board members, staff and students. The e-mail system may not be used for personal gain, political or religious activities or be used in any illegal, offensive or unethical manner. The email system is intended only for legitimate IPS-related communication, and any email communications to a student shall always originate from the employee's IPS email address and be directed to the student's IPS email address.

As a public institution, in accordance with law, all email communications originating in or received by the IPS email system in the transaction of official IPS business are open to public inspection by any citizen of the Ipswich community. All confidential information as defined by law contained in such email communications shall be redacted prior to public inspection and/or dissemination. Examples of confidential information that shall not be shared with the public include student education and health-related information made confidential by the Family Educational Rights and Privacy Act ("FERPA"), and information designated as confidential by any state or federal rule, regulation, or law.

IPS reserves the right to access employee email for any business purpose or for investigations related to potential disciplinary or legal action.

Social Media and Other Electronic Communication

Professional social media should be designed to support reasonable instructional, educational or extracurricular programs under the direct supervision of building and district administration. IPS Employees shall treat social media as a professional workplace. The same standards expected in IPS professional settings are expected in social media engagement. IPS employees who choose to engage in social media shall maintain a clear distinction between personal and

professional social media accounts. No school business shall be conducted over any social media account not associated with a district email address.

Professional Use of Social Media

Employees shall only use accounts associated with an IPS email address for professional social media activities. All professional social media accounts shall be associated with district provided and/or managed login credentials and shall conform to district-dictated privacy settings.

The district may log in to any employee's professional social media at any time. Employees shall not disclose any personally identifiable student information through social media outlets, including but not limited to student photographs, likenesses, recordings and creative works without expressed or implied consent on file.

Employees shall not disclose confidential information about staff through social media outlets. Employees are responsible for reporting inappropriate social media use to building administration

Personal Use of Social Media

Personal social media must be maintained separately from professional social media. Employees shall not use an IPS email address for any personal social media activity. IPS employees shall not communicate with any current IPS student through personal social media if that student is not a relative. If an employee receives a request from a current IPS student to connect or communicate through personal social media, he or she shall refuse the request. Employees shall not disclose any personally identifiable student information through personal social media outlets. Employees shall not access personal social media accounts during designated work hours.

Personal social media use has the potential to result in disruption of the workplace and can violate district policy and/or local, state, or federal law. In this event, administration may have an obligation to take appropriate investigative and/or disciplinary action concerning content of employee social media use.

Employee Use of Personal Devices

As a courtesy, IPS provides network connectivity to employees for personal devices through a Bring-Your-Own-Device wireless network. All traffic through this network is subject to inspection and no expectation of privacy should be assumed. Employees should keep personal use of devices to a minimum. Excessive use, as defined by district administration, is subject to disciplinary action. Employees shall not maintain student records, including but not limited to student photographs, likenesses, recordings and creative works, on personal devices.

Artificial Intelligence Tools

Employees may use artificial intelligence tools for legitimate IPS-related work without separate approval of each tool. Employees are expected to adhere to the [IPS AI Vision Statement](#) and must comply with this Agreement, applicable district policies and laws, and the tool's terms of use. This permission applies to employee use only and does not authorize software installation, the creation of student accounts, or student use of services outside established district procedures.

Employees shall not enter, upload, or otherwise disclose confidential, protected, or personally identifiable information to an AI tool unless the district has expressly approved that tool and its use with that type of information. Protected information includes, but is not limited to, identifiable student work, education and health records, grades, IEP or Section 504 information, photographs or recordings, employee records, account credentials, and district security information. Removing a person's name does not make information safe if the individual could still reasonably be identified. Employees remain responsible for any work they create, use, or share with the assistance of AI.

Copyright Policy

Employees shall model legal and ethical practice related to technology use just as they would for any other medium.

Internet Safety Training

All teachers, staff and administrators shall participate in annual Internet safety training. These trainings may include online modules, live trainings, or simulations.

Network Security and IPS Accounts

The IPS network and computer equipment may only be accessed by users with valid IPS network accounts. Employees shall only use their assigned network accounts when accessing the district network or when using machines or devices owned by IPS. Employees shall not provide their network password or account information to any group or individual other than authorized district personnel. Employees shall never allow another user access to a device currently logged into their own network account.

No alternative network shall be created or used by staff unless approved by the IT Department. "Alternative network" is defined as any wired or wireless network or sub-network located on or accessible from any IPS property that is not part of the primary network managed by the IT Department. Virtual Private Network (VPN) mobile applications or Virtual Private Network (VPN) software is not permitted unless approved or provided by the IT Department. Unless prior permission is obtained from IT, all network equipment must be approved and installed by IT Department staff.

Use of software or methods designed to gain passwords or digital access beyond the rights assigned to a user or device is prohibited. Use of such programs or methods risks the security

of the network and is a violation of district policy and federal law. If employees discover passwords or any other measure used to obtain unauthorized access to the IPS network, data, or applications, they shall report the discovery to their supervisor or IT.

No employee shall hide or attempt to hide files or folders stored on a network server or local workstation unless such action is approved by the IT Department administrative staff.

Employees do not have an expectation of privacy in using their IPS accounts. All IPS accounts may be monitored and searched at any time by authorized district personnel to protect the rights and property of IPS and ensure quality of service.

Workstation/Device Use

Employees are prohibited from installing any software on district-owned devices without district authorization. Employee use of any IPS device or service for illegal, obscene, pornographic, commercial, political or religious activity or for personal profit is prohibited. District-owned devices or devices are intended only for legitimate IPS work-related activities.

Changing or tampering with any IPS-owned device's system configuration is prohibited. Content is filtered for all users accessing the Internet through the IPS network. Any attempt to bypass the internet content filtering by use of a proxy, VPN or other means is prohibited unless such action is authorized by the IT Department.

Viruses and Virus Protection

IPS will install and maintain all virus protection and related software for district-owned equipment. The intentional spreading of messages or files containing damaging or destructive programs or data is against federal law. Violators will be prosecuted. Contact the IT Department immediately to report a device that may contain a virus or malware.