Long Prairie Grey Eagle Public Schools
Cyber Security Policy
July 2024

Introduction

Information Technology (IT) is an integral and critical component of Long Prairie Grey Eagle, (LPGE) daily business and educational needs. This policy seeks to ensure that LPGE's IT resources efficiently serve the primary business/educational functions of LPGE, provide security for LPGE and users electronic data, and comply with federal and other regulations. IT resources include hardware (computers, servers, peripherals), software (licensed applications, operating systems), network equipment (routers, firewalls, wiring), and IT personnel. The integrity of all IT resources is extremely important to the successful operation of LPGE.

All computer equipment, peripherals, and software are LPGE's property and are provided for business/educational purposes. Proper use and control of computer resources is the responsibility of all employees . Intentional or reckless violation of established policies or improper use of LPGE's computers will result in corrective action up to and including termination.

Employees should also be aware that any work completed on LPGE's computers is subject to monitoring and review, and they should not expect their communications to be private.

Policy Statement

It is the policy of LPGE Schools to use IT resources in a cost-effective manner that safeguards student and employee data and promotes accuracy, safety, Information, and efficiency. The overriding goal of this policy is to comply with all federal and other regulations and to protect the integrity of the private and confidential data that resides within LPGE's technology infrastructure.

Review and Acceptance

The School Board, Technology Director, and IT staff shall review this comprehensive policy at least annually, making such revisions and amendments as deemed appropriate and indicating approval and the date thereof in the policy header.

All LPGE staff are responsible for review and acceptance of this policy annually. Appropriate communications by way of a reminder will be sent by Administration or its assignee along with instructions for acceptance.

Acceptable Use of Information Systems

Definitions
Information Systems: All electronic means used to create, store, access, transmit, and use data, information, or communications in the conduct of administrative, instructional, research, or service activities. Additionally, it is the procedures, equipment, facilities, software, and data that are designed, built, operated, and maintained to create, collect, record, process, store, retrieve, display, and transmit information.

Authorized User: An individual or automated application or process that is authorized access to the resource by the system owner, in accordance with the system owner's procedures and rules.

Overview
Data, electronic file content, information systems, and computer systems at LPGE must be managed as valuable organization resources.

Information Technology's (IT) intentions are not to impose restrictions that are contrary to LPGE's established culture of openness, trust, and integrity. IT is committed to protecting LPGE's authorized users from illegal or damaging actions by individuals either knowingly or unknowingly.

Internet systems including, but not limited to, computer equipment, software, operating systems, storage media, network accounts providing electronic mail, WWW browsing, and File Transfer Protocol (FTP) are the property of LPGE. These systems are to be used for school purposes in serving the interests of LPGE and of its students.

Effective security is a team effort involving the participation and support of every LPGE employee, volunteer, and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines and to conduct activities accordingly.

Purpose
The purpose of this policy is to outline the acceptable use of computer equipment at LPGE. These rules are in place to protect the authorized user and LPGE. Inappropriate use exposes LPGE to risks including virus attacks, compromise of network systems and services, and legal issues.

Scope
This policy applies to the use of information, electronic and computing devices, and network resources to conduct LPGE business or interact with internal networks and business systems, whether owned or leased by LPGE, the employee, or a third party.

All employees, students, volunteers, contractors, consultants, subs, and other workers at LPGE, including all personnel affiliated with third parties, are responsible for exercising good judgment regarding appropriate use of information, electronic devices, and network resources in accordance with LPGE policies and standards, local laws, and regulations.

Policy Detail

Ownership of Electronic Files
All electronic files created, sent, received, or stored on LPGE-owned, leased, or administered equipment or otherwise under the custody and control of LPGE are the property of LPGE.

Privacy
Electronic files created, sent, received, or stored on LPGE-owned equipment, or otherwise under the custody and control of LPGE are not private and may be accessed by LPGE IT employees or administration at any time without knowledge of the user, sender, recipient, or owner. Electronic file content may also be accessed by appropriate personnel in accordance with directives from Human Resources or the Superintendent.

General Use and Ownership
Authorized users are accountable for all activity that takes place under their username.

Authorized users should be aware that the data and files they create on the school's systems immediately become the property of LPGE. Because of the need to protect LPGE's network, there is no guarantee of privacy or confidentiality of any information stored on any network device belonging to LPGE.

For security and network maintenance purposes, authorized individuals within the LPGE IT Department may monitor equipment, systems, and network traffic at any time.

LPGE's IT Department reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

LPGE's IT Department reserves the right to remove any non-business-related software or files from any system. Examples of non-business related software or files include, but are not limited to; games, instant messengers, pop email, music files, image files, freeware, and shareware.

System-level and user-level passwords must comply with the Password Policy. Authorized users must not share their LPGE login ID(s), account(s), passwords, Personal Identification Numbers (PIN) or similar information or devices used for identification and authentication purposes. Providing access to another individual, either deliberately or through failure to secure its access, is prohibited.

All PCs, laptops, and workstations should be secured with a password-protected screensaver with the automatic activation feature set at 10 minutes or less.

All users must lockdown their PCs, laptops, and workstations by locking (Windows + L) when the computer will be unattended for any amount of time.

All users are responsible for promptly reporting the theft, loss, or unauthorized disclosure of school information to their immediate supervisor and/or the IT Department.

All users must report any weaknesses in LPGE computer security and any incidents of possible misuse or violation of this agreement to their immediate supervisor and/or the IT Department.

Authorized users must use extreme caution when opening email attachments received from unknown senders, which may contain viruses or e-mail phishing attempts.

Unacceptable Use

Users must not intentionally access, create, store, or transmit material which LPGE may deem to be offensive, indecent, or obscene.

Under no circumstances is an employee or temporary employee of LPGE authorized to engage in any activity that is illegal under local, state, federal, or international law while utilizing LPGE-owned resources.

System and Network Activities

The following activities are prohibited by users, with no exceptions:

- Violations of the rights of any person or company protected by copyright, or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of “pirated” or other software products that are not appropriately licensed for use by LPGE.
- Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, email phishing, etc.).
- **Revealing your account password to others or allowing use of your account by others. This includes subs, student teacher assistants, paraprofessionals, family and other household members when work is being done at home.**
- Using a LPGE computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws.
- Attempting to access any data, electronic content, or programs contained on LPGE systems for which they do not have authorization, explicit consent, or implicit need for their job duties.
- **Installing any software, upgrades, updates, or patches on any computer or information system without the prior consent of LPGE IT.**
- **Installing or using non-standard shareware or freeware software without LPGE IT approval.**

- Installing, disconnecting, or moving any LPGE owned computer equipment and peripheral devices without prior consent of LPGE's IT Department.
- **Purchasing software or hardware, for LPGE use, without prior IT compatibility review.**
- Purposely engaging in activity that may; degrade the performance of information systems; deprive an authorized LPGE user access to a LPGE resource; obtain extra resources beyond those allocated; or circumvent LPGE computer security measures.

- Downloading, installing, or running security programs or utilities that reveal passwords, private information, or exploit weaknesses in the security of a system. For example, LPGE users must not run spyware, adware, password cracking programs, packet sniffers, port scanners, or any other non- approved programs on LPGE information systems. The LPGE IT Department is the only department authorized to perform these actions.

- Circumventing user authentication or security of any computer, network, or account.

- Interfering with, or denying service to, any user other than the employee's computer (for example, denial of service attack).

Access to the Internet at home, from a LPGE-owned computer, must adhere to all the same policies that apply to use from within LPGE facilities. Authorized users must not allow family members or other non-authorized users to access LPGE computer systems.

LPGE information systems or hardware must not be used for personal benefit. Examples include but not limited to: Selling products or merchandise, promoting non school related fundraising activities.

User Passwords

Passwords for LPGE network access must be implemented according to the following guidelines:

- Passwords must adhere to a minimum length of 10 characters
- Passwords must contain a combination of alpha, numeric, and special characters, where the computing system permits (!@#$%^&*_+=?/~';',<>|\).
- Passphrases are also encouraged. This could be as easy as using a sentence as your password.
- Passwords must not be easily tied back to the account owner such as: username, social security number, nickname, relative's names, birth date, etc.
- Passwords must not be dictionary words or acronyms
- Password changes may be required periodically.

Multi Factor Authentication

LPGE IT department will require Multi Factor Authentication on Google Apps (i.e. Email, Drive etc.) by September 30th 2022.

Employes will have two options to use for Multi Factor Authentication. (only need one of these)

- Personal Cell Phone Text Message
- Classroom Phone Number voice codes

Other district owned Software will be required to have Multi Factor Authentication as the software permits. (This is not available from Skyward at this time)

LPGE Wi-Fi Network

LPGE IT department will provide access to its secure wifi network on LPGE owned devices only.
LPGE also provides Guest Internet access to personal devices. This is a password protected network. The password will be posted in each building for Guest access. LPGE is not responsible for any damage to personal devices when using the Guest network. LPGE reserves the right to remove the Guest network or block access to users who are using the guest access in violation of policy.

Review and Acceptance

Each employee must complete a cyber security training program each school year or upon employment. This online training will be assigned and managed by the IT department. Training and assessment must be completed two weeks after the first workshop day. Failure to complete this training may result in the blocking of access to LPGE IT equipment.

Employees will be sent automated tests each month by email. These tests may include phishing attempts or other cyber security tactics to test each employee's understanding of security on IT equipment. The length of the test will be determined by how the employee handels the automated request. (For example, if a phishing email is sent to the user. The user deletes the message. That test is complete. If the user opens and responds to the phishing email they will be required to review material about phishing.)

If an employee fails two phishing tests they will be required to repeat the cybersecurity training within one week of notification from the IT team. Building level administration will be informed of the repeat training.

All LPGE staff are responsible for the review and acceptance of this policy. Acceptable use upon starting work at LPGE. New employee onboarding and training shall include this Policy at a minimum, and in addition to all other applicable training and orientation material, and instructions for acceptance shall be provided at that time. Signed acceptance will be received and retained by Information Technology management.

_____ Date:_____

LPGE Staff Member