PELHAM SCHOOL DISTRICT POLICY
GBEF-R – RESPONSIBLE USE OF TECHNOLOGY AGREEMENT FOR STAFF

The use of technology is a part of most employees' work in the Pelham School District School District. It is a privilege and must be respected and used wisely. The use of technology includes:

- Using both District-owned and personally-owned technology for school-related purposes, and
- Using any device to access a school network or the Internet through the school network, or to access District systems..

Technology in the Pelham School District is provided for school-related purposes, communication services, and business data services that support the mission, vision, core beliefs, and goals of the District.

The Pelham School District's Technology Responsible Use Agreement for Employees applies to all employees' use of all District and employee personally owned technology devices used while working. The expectations below provide appropriate and ethical use procedures for employees. They are not all-inclusive, as we cannot outline every possible permutation of employee behavior with technology. Some activities are expressly prohibited by law; other activities are inappropriate as defined by the administration of the District. Employee use of technology is the most powerful way we can foster ethical and appropriate student use.

We require employees to use technology in accordance with general expectations for appropriate employee behavior. Violation of any of these procedures will result in appropriate disciplinary action that may include a warning and/or dismissal. Additionally, violations will be referred to the police if appropriate.

Safety, Security and Privacy
- All accounts must be used solely by the designated user.
- All accounts must be used for school/work purposes and must be used in accordance with District Policy GBEF.
- Employees must keep their login and passwords personal and private.
- Employees must always logout of all devices before walking away so that their files, passwords, and network access is protected from abuse by others.
- Employees are expected to use appropriate judgement and caution in communications concerning students and staff to ensure that personally identifiable information remains confidential, and is not disclosed, used, or disseminated without proper authorization.
- Employees may post student produced material on the Internet only after administrative review and parental permission. At that point, it will be considered fair use and available to the public.
- Employee-produced material may be posted publicly. It is important that all content made available is created with professionalism and care. At that point, it will be considered fair use and available to the public.
- Employees must not attempt to alter data, the configuration of District technology, or the files of another user, without the consent of the individual, building administrator, or

technology administrator.
- Employees must not engage in any malicious use, disruption or harm to District technology or its network.
- Employees must not use or possess software that can be used for hacking, eavesdropping, network administration/monitoring, virus creation or propagation or network security circumvention.
- Employees agree to report any misuse or abuse of the District's technology to the District's network administrator.
- Data stored on any District technology and in the District's learning management system account is not private. Pelham School District personnel have the right to review all data, email, logs or files that exist on the network or individual systems without prior consent of the user.

Online Behavior
- School-related use of technology devices always takes priority over personal use of technology devices.
- Employees should use the District's learning management system account for all correspondence related to their work.
- Employees' use of email, texting, chat, instant messaging, and/or social media must be only for appropriate, legitimate, and responsible communication. Its use is to be approved by the supervisor.
- Employees are reminded that personal postings on the Internet may be shared without the owner's knowledge, and could become viewable by unintended audiences such as students, parents, employers and members of the community. Additionally, employees are reminded that audiences may not be able to distinguish between professional and personal posts in social media.

Cyberbullying and Inappropriate Materials
- Employees must not use any device to bully others. These violations will be handled in accordance with the Pelham School District Policy JICK Pupil Safety and Violence Prevention.
- Employees must not create, access, download, edit, view, store, distribute, display, or print materials or messages that are illegal, harassing, intimidating, discriminatory, defamatory, sexually explicit, obscene, violent, or pornographic.
- Employees must not attempt to defeat or bypass the District Internet filters that are in place to block inappropriate content or to conceal inappropriate activity. Employees who believe filtering should be disabled or made less restrictive for their own temporary, bona fide research or other lawful purposes should discuss the matter with their building administrator.
- Employees must notify school administrators if they become aware of illegal or inappropriate behavior.

Other
- Employees are expected to take appropriate care of District technology when using and transporting them.
- Employees are responsible for compensating the school for any losses, cost or damages incurred by the school for violations of the Board policies and school rules while the employee is using District technology including the cost of investigating such violations. The District assumes no responsibility for any unauthorized charges or costs incurred by an employee while using school computers.
- Employees are asked to consider the amount of printing. Use digital platforms and distribution channels to save paper.
- Employees using specialized technology that needs to be backed up are responsible for backing up their data. The District is not responsible for any data loss. Employees are encouraged to upload their data files to their cloud-based drive.
- Except in the performance of their duties as school employees, employees are prohibited from sending email messages to groups of school employees using their school email or other emails without permission of the building administrator or Superintendent. Prohibited uses of the email system also include but are not limited to:
  - Solicitation of membership in any non-school-sponsored organization;
  - Advocacy or expression by or on behalf of individuals or non-school-sponsored organization;
  - Political or religious purposes;
  - Raising funds for non-school-sponsored purposes, whether profit-making or not for profit;
  - Selling articles or services of any kind, advertising or promoting any kind of business;
  - Any communications that represent an employee's views as those of the District or that could be misinterpreted as such.

Discipline Consequences
Responsible and appropriate behavior is expected of all users. Violation of any guidelines will result in appropriate disciplinary action up to and including dismissal. The school administration has the right to assign the consequence based on the severity of the violation. Behaviors that will result in a consequence include but not limited to:
- Use of another person's login, or password to access the network, Internet or user files.
- Use of the Internet to access depictions that are obscene, violent or pornographic or are of a harmful nature to minors.
- Use of the Internet for non-work related purposes that are detrimental to bandwidth and inappropriate for a professional setting.
- Use of inappropriate screensavers, backgrounds or inappropriate pictures on your device.
- Inappropriate use of email, texting, chat and/or social media.
- Damage or abuse of another person's device.
- Leaving a device unattended and/or not secured in a public area.
- Failing to return a school district owned device when required.

- Hacking (intentional misuse or abuse of computer facilities) can be considered a felony and subject to cancellation of all technology privileges and appropriate disciplinary action.
- Disruption of school computer systems and/or network, including bypassing or changing restrictions or settings.
- Overriding the District's Internet filter, use or accessing proxies.
- Destruction of District technology.
- Engaging in any activities that are in violation of the District's Pupil Safety and Violence Prevention policy. (JICK)

School District Rights

The District reserves the right to:

1. Monitor all activity. Notwithstanding any related laws, staff members have no expectation of privacy regarding their use on the school district computer network.
2. Make determinations on whether specific uses of a network are consistent with these acceptable use procedures.
3. Log and monitor network utilization by users.
4. Determine what is appropriate use.
5. Remove a user's access to the network at any time it is determined that the user engaged in unauthorized activity or violated these acceptable use procedures.
6. Cooperate fully with any investigation concerning or relating to the District's network activity.

PELHAM SCHOOL DISTRICT POLICY
GBEF-R – RESPONSIBLE USE OF TECHNOLOGY AGREEMENT FOR STAFF

It is the responsibility of the user to familiarize him/herself with and abide by the rules of this Responsible Use Agreement for Employees.

I hereby certify that I have read the Responsible Use Agreement for Employees; that I fully understand their terms and conditions; and that I will abide by the terms conditions set forth in this document.

Name of user: _____

Home phone: _____

Position /Assignment:_____

Signature of user: _____

Date: _____

Signature of Building Principal:_____

Date: _____