RESOLUTION NO: 22-26
OF THE CITY OF FRANKLIN, INDIANA
COMMON COUNCIL

RESOLUTION ADOPTING ACCEPTABLE USE POLICY

This resolution dated the 17th day of October, 2022 by the Common Council for the City of Franklin as follows:

WHEREAS, the City of Franklin, Indiana, by and through its Board of Public Works and Safety and the Common Council is responsible for adopting policies for its employees and the funding and supplying the acquisition of City property; and

WHEREAS, the City of Franklin Telecommunications Council was tasked with revising and establishing an Acceptable Use Policy governing the manner in which employees should use the City's information technology; and

WHEREAS, the City of Franklin Telecommunications Council has unanimously created said Acceptable Use Policy as set forth on the attached Exhibit "A"; and

WHEREAS, on September 21st, 2015 the City of Franklin adopted an Employee Handbook in which every employee is expected to comply with the rules and policies set forth therein; and

WHEREAS, the Acceptable Use Policy developed by the Telecommunications Council is intended to become a part of the Employee Handbook and all employees shall comply with the policies, procedures and practices set forth in the Acceptable Use Policy as outlined on the attached Exhibit "A";

NOW THEREFORE BE IT RESOLVED that the Common Council does find it is in the best interest of the citizens of Franklin and the City employees that the Acceptable Use Policy be adopted in its entirety.

BE IT FURTHER RESOLVED that the Common Council of the City of Franklin does determine that the Acceptable Use Policy as set forth on the attached Exhibit "A" should be adopted and incorporated into the City Employee Manual.

BE IT FURTHER RESOLVED that the Common Council does authorize and approve the adoption of the Acceptable Use Policy per the attached Exhibit "A" and that said policy shall be incorporated in full in the Employee Handbook of the City of Franklin.

BE IT FURTHER RESOLVED that the Acceptable Use Policy identified on attached Exhibit "A" supersedes all prior inconsistent policies, procedures and practices, both verbal or written.

BE IT FURTHER RESOLVED that all prior policies set forth in the City Employee Manual NOT inconsistent with the policies, procedures and practices established in the Acceptable Use Policy shall remain in full force and effect.

IT IS FURTHER RESOLVED that a copy of the Acceptable Use Policy shall be provided to each Department Head who will then provide a copy to all employees within their respective departments.

IT IS FURTHER RESOLVED that this Resolution shall be in full force and effect from and after the adoption of this Resolution and approval of the Resolution by both the Board of Public Works and Safety and the Franklin Common Council.

INTRODUCED & APPROVED by the Common Council of the City of Franklin, Johnson County, Indiana this 17th day of October, 2022.

City of Franklin, Indiana, by its Common Council:

Voting Affirmative:	Voting Opposed:
Kenneth Austin, President	Kenneth Austin, President
Jennifer Price	Jennifer Price
Absent Robert D. Heuchan	Robert D. Heuchan
Anne McGuinness	Anne McGuinness
Irene Nalley	Irene Nalley
Josh Prine	Josh Prine
Shawn Taylor	Shawn Taylor

Attest: Jayne Rhoades

Jayne Rhoades,
City Clerk Treasurer

Presented by me to the Mayor of the City of Franklin for his approval or veto pursuant to Indiana §36-4-6-15, 16 this 17 day of October, 2022 at 6:10 o'clock P.M.

Jayne Rhoades

Jayne Rhoades,
City Clerk Treasurer

This Ordinance having been passed by the legislative body and presented to me was Approved by me and duly adopted, pursuant to Indiana Code §36-4-6-16(a)(1) Vetoed pursuant to Indiana Code § 36-4-6-16(a)(2), this 17 day of October, 2022 at 6:10 o'clock P.M.

Steve Barnett, Mayor

Attest:

Jayne Rhoades

Jayne Rhoades,
City Clerk Treasurer

Prepared by:
Lynnette Gray, City Attorney

Acceptable Use Policy

Data Security

Encryption

All encryption technologies and techniques used must be approved by IT Management. The use of proprietary encryption algorithms is not permitted, unless approved by IT Management. IT Management is responsible for the distribution and management of all encryption keys. IT Management will create and publish City of Franklin Encryption Standards. Use of encryption should be managed in a manner that allows designated personnel prompt access to all data. Confidential data should only be stored on devices that are encrypted.

No expectation of privacy

Review of all log files and data by IT Management is standard practice and will occur periodically. There should be no expectation of privacy when using City owned devices or infrastructure including access to the Internet. Use of personally-owned devices does not imply a right to privacy.

Data exfiltration

Information created or stored on the City's assets will remain the property of the City of Franklin. The City owns the data, files, and content regardless of the creator/author. Copying, moving, or modifying data or files without the intent to add value or security to the City of Franklin, is against this policy and may result in disciplinary action including and not limited to termination of employment.

Multi-Factor Authentication (MFA)

Multi-factor authentication provides a second layer of security to any type of login, requiring extra information or a physical device to log in, in addition to your passphrase.

The City has established a Multi-Factor Authentication process, which provides a common method of protection for the City of Franklin. All individuals will be required to engage in one additional step for authentication.

Personally Identifiable Information (PII)

The Department of Labor definition of PII is as follows: Any representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means.

Least privilege:
To ensure minimal access to PII, access is only provided to City employees, contractors and vendors as required in the performance of their role. Any external transmission of PII must be encrypted.

Acceptable Use

With new technological advances it is easy for individuals to inadvertently fall victim to highly sophisticated phishing attacks. This could give a hacker unauthorized access to our network and information system (Network). IT Management has taken several steps to protect and monitor the network. An intentional disruption to the network or digital resources may result in disciplinary action.

Passwords

Many of the Information Systems used by the City require passwords. User's passwords should NEVER be shared with anyone, including members of IT Management, nor should any efforts be made to obtain the password of another user. If anyone requests your password, this activity should be reported to IT Management.

Email

Using a City issued email address for personal use is prohibited and may be the subject of disciplinary action. Email filtering and monitoring by IT Management is in place to protect the assets of the City.

Employees must adhere to this policy at all times, in addition to our confidentiality and data protection guidelines.

Anything sent via email that is PII or confidential must be encrypted. Note, any encryption processes must involve IT Management. See Data Security → Encryption.

Personal Equipment

Equipment not owned by the City (gaming systems, personal computers, printers, etc) cannot be physically plugged into the network. These systems must only be connected to the public

wifi. It may also be necessary to limit access speeds to ensure bandwidth is available for City purposes.

Cybersecurity

Training

Required quarterly training will inform employees of cybersecurity risks and safety measures. Additional training may be necessary as determined by IT Management. All employees must complete the required training within the specified deadline and understand their cybersecurity role and responsibilities. Certain tests will be completed by IT Management.

Overall, cybersecurity training is an essential part of the City's risk reduction effort. This will require clear connections between cybersecurity training and the business goals that it supports. It's vital to remember that cybersecurity in the workplace is everyone's responsibility: Training programs shall stress how individual employees can influence the overall security environment at an organization. The cybersecurity training will foster a culture that is cybersecurity literate and helps ensure organization-wide data security.

Cell phones

Screen Locks Are Mandatory
A screen lock is required to be in place on a cell phone prior to accessing the City's resources (i.e. network, email, apps, etc) regardless of the cell phone being owned by an individual or the City. Screen locks can consist of trace patterns, passwords, fingerprints, facial recognition, and even eye (iris) recognition technologies. The City may require additional authentication methods.

Wherever possible, be sure to use two-factor authentication as this adds another layer for the entry process.

Avoid Connecting to Open or Free WiFi Networks
This tip is the standard best practice for all computers and mobile devices. Public or open WiFi networks pose a particular threat to mobile devices. Instead of relying on WiFi, use your data plan to access the internet when you are without access to the city's network.

General

- Never leave computers unattended while logged-in.
- It is forbidden to install hubs, switches, Wi-Fi equipment, or any kind of hardware or software devices with the intent to duplicate and/or share access to the City's network.
- The City's network cannot be used for any commercial purposes.
- Falsifying or otherwise misrepresenting one's identity via email or any other form of communication is a violation of law. The unauthorized use of other user accounts is prohibited.
- Any unauthorized attempt to access or interfere with another computer and/or breach users' privacy is prohibited.