ORDINANCE NUMBER 8 - 2024

COUNTY OF FRANKLIN, KENTUCKY

AN ORDINANCE AMENDING THE OTHER COUNTY POLICIES SECTION OF CHAPTER 30: ADMINISTRATIVE CODE OF THE FRANKLIN COUNTY CODE OF ORDINANCES TO REMOVE AND ADD LANGUAGE UNDER SUBSECTIONS §30.170, §30.171, §30.172, §30.173, AND §30.174, (A), (B), (C), (D), (E), (F), (G), (H), (I), (J), (K), (L) and (M).

WHEREAS, The Franklin County Fiscal Court adopted the General Administration Section of Chapter 30: Administrative Code by Ordinance No. 1-2021 on the 19th day of February, 2021, to establish procedures and processes relating to the Constitutional office of the Franklin County Judge Executive; and

WHEREAS, the Judge Executive has established an Administrative Service Committee consisting of two Magistrates and the Judge Executive to consider amendments to the Administrative Code; and

WHEREAS, The Administrative Service Committee has met and considered changes relating to the General Administrative Section of Chapter 30: Administrative Code of the Franklin County Code Ordinances relating to the office of Judge Executive; and

WHEREAS, the Administrative Service Committee desires consideration by the Fiscal Court the General Administrative Section of Chapter 30: Administrative Code of the Franklin County Code Ordinances relating to the office of Judge Executive

NOW, THEREFORE, BE IT ORDAINED BY THE FISCAL COURT OF THE COUNTY OF FRANKLIN, COMMONWEALTH OF KENTUCKY, THAT:

SECTION I. The Code of Ordinances, Administrative Code, Chapter 30, §30.170 (A), (B), AND (C):

§ 30.170 EQUAL OPPORTUNITY.

(A) General policy. It has been, and will continue to be, the policy of the county to recognize and abide by the provisions of Title VI of the Civil Rights Act of 1964, being 42 U.S.C. §§ 2000d et seq., Title VIII of the Civil Rights Act of 1968, being 42 U.S.C. §§ 1404a et seq. and Executive Order 11246 of September 24, 1965 (30 F.R. 12319, 12935, 3 C.F.R. 1964-1965 Comp., p. 339) and amendments thereof.

(B) Equal Opportunity Officer.

(1) A member of the staff of the county shall be appointed by the County Judge/Executive to serve the functions of the Equal Opportunity Officer.

(2) The responsibilities of the officer shall include, but not be limited to, the following:

(a) Consult with and advise on matters pertaining to the administration of an equal opportunity program for the county staff;

(b) As assigned, establish and maintain contact as the county's liaison with the community generally and minority groups in particular;

(c) As assigned, work with schools, minority group agencies and organizations to encourage and assist with implementing equal opportunity in employment, training, housing and business development as pertains to the programs carried out by the county;

(d) Obtain information about human rights programs of federal, state and local agencies as well as special interest groups promoting equal opportunity for all the citizens of the county;

(e) Prepare reports, as needed, on equal opportunity practices and programs;

(f) Maintain liaison and continuing working relationships with state officials on equal opportunity;

(g) Review and monitor all contractual agreements with the county to assure achievement of equal employment opportunity, open occupancy and public accommodation objectives;

(h) Assist the county and contractors in preparing effective program criteria; compile public information for the county to disseminate; implement equal opportunity policies and statements; and prepare related correspondence including recommendations on equal opportunity practices; and

(i) Investigate formal complaints of alleged discrimination by parties to agreements and recommend procedures to ensure compliance with all county activities for the promotion of equal opportunity objectives.

(C) County staff. The county has taken, and will continue to take, steps to assure non-discrimination in its employment practices, including hiring, compensation, working conditions, promotions, demotions and terminations of its employees. Overt efforts will continue to be made to provide opportunities for equal employment and equal compensation within the county staff.

~~SECTION II. The Code of Ordinances, Administrative Code, Chapter 30, §30.171 (A), and (B)~~

~~§ 30.171 COUNTY INVESTMENT POLICY.~~

~~(A) The Fiscal Court of the county hereby adopts the following investment policy and strategy with respect to the investment of all funds, as required by KRS 66.480.~~

~~(B) The county authorizes the following to invest the county's funds, pursuant to the terms and conditions of Res. 20 (1994 Series):~~

~~(1) Funds not needed for current expenses or obligations of the county may be invested in any of the following:~~

~~(a) Obligations of the United States and of its agencies and instrumentalities, including obligations subject to repurchase agreements; provided that, delivery of these obligations subject to r-epurchase agreements is taken either directly or through an authorized custodian. The investments may be accomplished through repurchase agreements reached with sources including, but not limited to, national or state banks chartered in the commonwealth;~~

~~(b) Obligations and contracts for future delivery or purchase of obligations backed by the full faith and credit of the United States or a United States Government agency, including, but not limited to:~~

~~1. United States Treasury;~~

~~2. Export-Import Bank of the United States;~~

~~3. Farmers Home Administration;~~

~~4. Government National Mortgage Corporation; and~~

~~5. Merchant Marine bonds.~~

~~(c) Obligations of any corporation of the United States government, including, but not limited to:~~

~~1. Federal Home Loan Mortgage Corporation;~~

~~2. Federal Farm Credit Banks;~~

~~3. Bank for Cooperatives;~~

4. Federal Intermediate Credit Banks;

5. Federal Land Banks;

6. Federal Home Loan Banks;

7. Federal National Mortgage Association; and

8. Tennessee Valley Authority.

(d) Certificates of deposit issued by or other interest-bearing accounts of any bank or loan institution which are insured by the Federal Deposit Insurance Corporation or similar entity permitted by KRS 41.240(4);

(e) Uncollateralized certificates of deposit issued by any bank or savings and loan institution rated in one of the three highest categories by a nationally recognized rating agency;

(f) Bankers' acceptance for banks rated in one of the three highest categories by a nationally recognized rating agency;

(g) Commercial paper rated in the highest category by a nationally recognized rating agency;

(h) Bonds or certificates of indebtedness of this commonwealth and of its agencies and instrumentalities; and

(i) Securities issued by a state or local government, or any instrumentality or agency thereof, in the United States, and one of the three highest categories by a nationally recognized rating agency.

(2) The investment authority outlined above shall be subject to the following limitations:

(a) The amount of money invested at any time by the county in one or more of the categories outlined above shall not exceed 20% of the total amount of money invested by the county;

(b) The county shall not purchase any investment on a margin basis or through the use of any similar leveraging technique; and

(c) The county shall not purchase any investment where the principal funds are at risk or loss.

(3) The county hereby adopts the following standards for written agreements pursuant to which investments are made.

(a) The Fiscal Court should determine who is authorized to sign the written agreement, whether that agreement needs to be signed by more than one party, whether the agreement as whole will need to be approved by the Fiscal Court.

(b) The county should include any other requirements that it may want to make as a standard for the written agreement.

(4) The county hereby adopts the following procedures for monitoring controls, deposit or retention of investments and collateral:

(a) Working with the county's investment advisor, the county should make such determinations as to how often a report will be received on its deposits;

(b) Where the deposits or investments will be physically located;

(c) Whether a third-party custodian is desired or required for the collateral;

(d) Whether the county actually wants to take possession and control of the investment security or if that will be left with the county's bank/trustee; and

(e) The county should include any additional controls recommended by the investment advisor or the County Auditor.

(5) The county hereby adopts the following standards for diversification investments, including diversification with respect to the types of investments and firm with which the county transacts business: the county will determine how much of the investment should be in any one type of investment and how all transactions are to be executed.

(6) The county shall use the following standards for the qualification of investment agents authorized to transact business with the county: the Fiscal Court should determine what criteria to use in selecting an investment advisor, such as licensing to do business in the commonwealth, the investment advisor's experience, the capitalization of the investment advisory or any other prudent factors the Fiscal Court deems appropriate in its determination of whether a particular firm is capable and qualified to transact business with the county.

(7) All the county's investment reports will be prepared and submitted on a quarterly basis by the County Treasurer.

SECTION III. The Code of Ordinances, Administrative Code, Chapter 30~~, §30.172 (A), (B), and (C),~~ §30.171 (A), (B), and (C) is hereby amended to read as follows:

~~§ 30.172~~ § 30.171 DEPARTMENT OF PLANNING, ZONING AND BUILDING CODE ENFORCEMENT.

(A) Purpose. In order to ensure that all persons are treated equally and fairly, the following policies have been adopted to outline how, when and in what manner electrical and building construction projects will be conducted.

(B) Electrical inspections.

(1) All electrical installations require an electrical permit to be issued.

(2) Only electrical contractors currently licensed by the county, with current workers' compensation and liability insurance (see homeowner exception) may file for an electrical permit.

(3) If a building permit is required for the construction, no electrical inspection can be scheduled or completed until such time as the building permit is issued.

(4) Inspections will be scheduled on a first-come, first-served basis.

(5) With the exception of commercial and industrial projects, which are billed to electrical contractors after completion of the project, no inspection will be performed until the required inspection fee has been paid. See fee schedules for applicable fees.

(6) If an electrical inspection is disapproved, the electrician or property owners, performing their own work, will be required to pay the applicable reinspection fee. See fee schedules for applicable fee.

(7) No project will be scheduled for a reinspection, if it was previously denied, until the reinspection fee has been paid.

(8) On single-family and duplex construction, no temporary for service only inspections will be performed. At the time the final inspection is completed and approved, the certificate of compliance will be sent to the applicable utility company for hook-up.

(9) If work, which is required to be inspected, is covered prior to the inspection, the Planning and Building Codes office will fail the inspection and will require that all work be removed so that the inspection can be made. In this event, a reinspection fee will be required to be paid prior to the Planning and Building Codes Office scheduling the reinspection.

(10) All electrical inspections will be performed using the National Electrical Code, edition adopted by the Department of Housing, Buildings and Construction.

(11) Homeowners performing their own electrical work on the residence, in which they live, may perform their own electrical work and may apply for an electrical permit from the Office of Planning, Zoning and Building Code Enforcement. The homeowner is also required to file an affidavit certifying that they are performing their own work.

(C) Building inspections.

(1) No building inspection will be scheduled until such time as the building permit has been issued and obtained by the contractor or property owner.

(2) All inspections will be scheduled on a first-come, first-served basis.

(3) At the time the footer inspection is made, all property pins shall be in place and string lines run so that it can be determined that the building setback lines are in conformance with the subdivision plat or zoning ordinance.

(4) Letters from engineers certifying the construction of the footer and the zoning setback lines will not be accepted, unless an inspection has been scheduled, and our office fails to notify the property owner or contractor that the inspection cannot be made. Letters from engineers will be accepted only if the Planning and Building Codes Office requests it when there is a disagreement on whether the structure meets the required setbacks and the Planning and Building Codes Office agrees to accept an engineer's or surveyor's survey showing compliance with the required zoning setback lines.

(5) Contractors or property owners, or their agents, are required to meet the inspector on the site at the time of the inspection.

(6) A set of the construction plans, approved by the Department of Planning, Zoning and Building Code Enforcement, will be required to be on the site at the time of inspection.

(7) Framing and final inspections will be scheduled only after both electrical and plumbing inspections have been approved.

(8) If an inspection is disapproved, the contractor or property owner will be required to pay the applicable reinspection fee. (See fee schedules.)

(9) No reinspection will be scheduled until such time as the reinspection fee has been paid.

(10) No structure shall be occupied, wholly or in part, unless and until a certificate of occupancy has been issued by the Department of Planning, Zoning and Building Code Enforcement.

(11) If work, which is required to be inspected, is covered prior to the inspection, the inspector for the Planning and Building Codes office will fail the inspection and will require that all work be removed so that the inspection can be made. In this event, a reinspection fee will be required to be paid prior to the Planning and Building Codes Office scheduling the re-inspection.

(12) At the time the application for building permit is made, the applicant will be required to choose which code (Kentucky Building Code or ~~CABO One- and Two-Family Dwelling Code~~ the Kentucky Residential Code) by which the construction project will be reviewed and inspected.

SECTION IV. The Code of Ordinances, Administrative Code, Chapter 30, ~~§30.173 (A), (B), (C), (D), (E), (F), (G), and (H)~~ §30.172 (A), (B), (C), (D), (E), (F), (G), and (H) is hereby amended to read as follows:

~~§ 30.173~~ -§ 30.172 ACCEPTABLE USES OF THE INTERNET AND COUNTY E-MAIL.

(A) General. Each county employee and official shall be issued an official county e-mail address, which shall be used and maintained for all official business and correspondence of county government.

(B) Acceptable uses of the internet and county e-mail. The county-provided internet and e-mail access is intended for business purposes only. The county encourages the use of the internet and e-mail because it makes communication more efficient and effective. However, internet service and e-mail are county property, and their purpose is to facilitate county business. Every user has a responsibility to maintain and enhance the county's public image and to use county e-mail and access to the internet in a productive manner. To ensure that all users are responsible, the following guidelines have been established for using e-mail and the internet. Any improper use of the internet or e-mail is not acceptable and will result in appropriate disciplinary action, up to and including dismissal.

(C) Unacceptable uses of the internet and county e-mail. The county internet and e-mail access may not be used for transmitting, retrieving or storage of any communications of a discriminatory or harassing nature or materials that are obscene or X-rated. Harassment of any kind is prohibited. No messages with derogatory or inflammatory remarks about race, age, disability, religion, national origin, physical attributes or sexual preference shall be transmitted. No abusive, profane or offensive language is allowed to be transmitted through the county's e-mail or internet system. Electronic media may not be used for any purpose which is illegal, deceptive or against county policy or contrary to the county's best interest. Use of county e-mail or internet for personal gain is prohibited.

(D) Communications.

(1) Each user is personally responsible for the content of all test, audio or images that he or she places or sends over the county's e-mail/internet system. No e-mail or other electronic communications may be sent which hides the identity of the sender or represents the sender as someone else or someone from another entity. All messages communicated on the county's e-mail/internet system should contain the user's name. Excessive personal communications are prohibited. Any messages or information sent by a user to another individual outside the county via an electronic network (e.g., bulletin board, online service or internet) are statements that reflect on the county. While some users include personal "disclaimers" in electronic messages, there is still a connection to the county and the statements may be tied to the county.

(2) All communications sent by users via the county's e-mail/internet system must comply with this and other county policies and may not disclose any confidential or proprietary information.

(E) Downloading and installing software. To prevent computer viruses from being transmitted through the county's e-mail/internet system, there will be no unauthorized downloading of any unauthorized software. All software downloaded must be registered to the county. Users should contact the County Judge/Executive if they have any questions.

(F) Copyright issues. Copyrighted material belonging to entities other than the county may not be transmitted by users on the county's e-mail/internet system. All users obtaining access to other companies' or individuals' materials must respect all copyrights and shall not copy, retrieve, modify or forward copyrighted materials, except with permission, or as a single copy, to reference only. Failure to observe copyright or license agreements may result in disciplinary action up to and including termination.

(G) Security. The county routinely monitors usage patterns for its e-mail/internet communications. The reasons for this monitoring are many, including cost analysis/allocation and the management of the county's gateway to the internet. All messages created, sent or retrieved over the county's e-mail/internet are the property of the county and may be considered public information. The county reserves the right to access and monitor all messages and files on the county's e-mail/internet system. Users should not assume electronic communications are totally private and should transmit highly confidential data in other ways. Passwords and sign-on access codes shall not be shared with anyone including co-workers, family members or other unauthorized personnel. A user will be designated as system administrator for e-mail/Internet purposes. Users shall minimize the risk of disclosing personal information via electronic or other means. For more details, see § 30.174 of this chapter.

(H) Violations. Any employee who abuses the privilege of county-facilitated access to e-mail or the internet will be subject to corrective action up to and including termination. If

necessary, the county reserves the right to advise appropriate officials of any suspected illegal violations.

SECTION V. The Code of Ordinances, Administrative Code, Chapter 30, ~~§30.174 (A), (B), (C), (D), (E), (F), (G), (H), (I), (J), (K), (L), and (M)~~ §30.173 (A), (B), (C), (D), (E), (F), (G), (H), (I), (J), (K), (L), and (M) is hereby amended to read as follows:

~~§ 30.174~~ § 30.173 PROTECTION OF PERSONAL INFORMATION.

(A) Definition. PERSONAL INFORMATION means an individual's first name or first initial and last name; personal mark; or unique biometric or genetic print or image, in combination with one or more of the following data elements:

(1) An account number, credit card number or debit card number that, in combination with any required security code, access code or password, would permit access to an account;

(2) A Social Security number;

(3) A taxpayer identification number that incorporates a Social Security number;

(4) A driver's license number, state identification card number or other individual identification number issued by any agency;

(5) A passport number or other identification number issued by the United States government; or

(6) Individually identifiable health information as defined in 45 C.F.R. § 160.103, except for education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. § 1232g, 34 C.F.R. Part 99.

(B) Policy overview.

(1) The purpose of this policy is to minimize the risk of disclosing personal information and setting practical guidelines for effectively responding to security incidents. This policy sets forth the procedures and practices pursuant to KRS 61.932. In addition, this policy requires appropriate measures to protect information stored on media, both digital and non-digital, during the entire term of its use, until its destruction.

(2) Non-digital media containing personal information shall be physically controlled and securely stored in a manner meant to ensure that the media cannot be accessed by unauthorized individuals. This may require storing media in locked containers such as cabinets, drawers, rooms or similar locations if unauthorized individuals have unescorted

access to areas where personal information is stored. If personal information is stored in an electronic format, it shall be protected from access by unauthorized individuals. Such information must be protected by software that prevents unauthorized access. If personal information is transmitted via e-mail or other electronic means, it must be sent using appropriate encryption mechanisms.

(3) All personal information shall remain secure and, when applicable, non-digital media shall be appropriately disposed. Non-digital media containing personal information must be properly stored and secured from view by unauthorized persons.

(C) Point of contact. The Judge/Executive shall designate a point of contact ("POC"). The POC shall serve the following functions:

(1) Maintain the adopted information security policy and be familiar with its requirements;

(2) Ensure that employees and others with access to personal information are aware of and understand the information security policy;

(3) Serve as contact for inquiries from other agencies regarding its information security policy and any incidents;

(4) Be responsible for ensuring compliance with the information security policy; and

(5) Be responsible for responding to any incidents.

(D) Security software.

(1) Security software used to protect personal information must provide user identification, authentication, data access controls, integrity and audit controls.

(2) Security software should be adequately tested to confirm functionality and to ensure that it is minimally disruptive to all associated operating systems, communications, applications and other associated software systems. Contractual provisions must also ensure that the supplier's software, by design or configuration, will not introduce any security exposures.

(3) The level of protection afforded by security software should be commensurate with the sensitivity of the data. For example, if data resides in a database that is deemed highly confidential, stringent access controls to the database should be employed. The level of protection along with the methods to implement that protection should be addressed before any personal information is stored on a device.

(4) Systems, networks and application software used to process personal information must adhere to the highest level of protection reasonably practical. Intrusion detection and prevention software shall be used.

(E) Encryption. Information stored on digital media shall be encrypted in accordance with contemporary standards.

(F) Access control. Only authorized individuals are permitted access to media containing personal information. In addition to controlling physical access, user authentication should provide audit access information. Any access must comply with applicable regulatory requirements.

(G) Portable computing devices.

(1) This policy prohibits the unnecessary placement (download or input) of personal information on portable computing devices. However, users who in the course of business must place personal information on portable computing devices must be aware of the risks involved and impact to the affected person/entities in the event of actual or suspected loss or disclosure of personal information. If personal information is placed on a portable computing device, reasonable efforts must be taken, including physical controls and encryption, to protect the information from unauthorized access.

(2) Additionally, each person using the portable computing device must sign the county e-mail and internet user agreement form indicating acceptance of the information and acknowledging his or her understanding of the responsibility to protect the information. In the event the portable computing device is lost or stolen, the user should be able to accurately recreate the personal information and must be able to provide notification to all affected persons/entities.

(3) When it is determined that personal information must be placed on a portable computing device, every effort should be taken to minimize the amount of information required. If possible, information should be abbreviated to limit exposure (e.g., last four digits of the Social Security number).

(H) Physical security procedures.

(1) This policy section is to ensure that its information resources are protected by physical security measures that address physical tampering, damage, theft or unauthorized physical access. Access to restricted areas containing information technology resources or other sources of personal information shall be limited to authorized personnel only.

(2) When feasible, information technology equipment should be marked with some form of identification that clearly indicates it is the property of the county. During transport, media shall be protected and controlled outside of secured areas and activities associated with

transport of such media restricted to authorized personnel. Tracking methods shall be developed and deployed to ensure media reaches its intended destination.

(I) Types of incidents. Threats to the security of personal information arise in many different ways. Attacks on personal information may arise from:

(1) External/removable media: an attack executed from removable media (e.g., flash drive, CD) or a peripheral device;

(2) Attrition: an attack that employs brute force methods to compromise, degrade or destroy systems, networks or services;

(3) Web: an attack executed from a website or web-based application;

(4) E-mail: an attack executed via an e-mail message or attachment;

(5) Improper usage: any incident resulting from violation of an organization's acceptable usage policies by an authorized user, excluding the above categories;

(6) Loss or theft of equipment: the loss or theft of a computing device or media used by the organization, such as a laptop or smart phone; and

(7) Other: an attack that does not fit into any of the other categories.

(J) Destruction of records containing personal information.

(1) A media retention schedule shall be defined for all media in accordance with regulatory requirements. The Fiscal Court shall have a document/information retention policy. When records containing personal or confidential information are ready for destruction, they shall destroy the information completely to ensure that the information cannot be recognized or reconstructed. In addition, any personal or confidential data contained on the computer media must be obliterated and/or made indecipherable before disposing of the tape, diskette, CD-ROM, zip disk or other type of medium.

(2) Appropriate methods and equipment must be used to routinely destroy personal or confidential information. One of the following safeguards must be implemented:

(a) Hire a document disposal contractor to dispose of the material. The contractor should be certified by a recognized trade association and should use disk sanitizing software and/or equipment approved by the United States Department of Defense. The company's information security policies and procedures shall be reviewed and evaluated. Additionally, documents shall be reviewed such as an independent audit of a disposal company's operations and/or its compliance with nationally recognized standards;

(b) Secure and utilize shredding equipment that performs cross-cut or confetti patterns;

(c) Secure and utilize disk sanitizing or erasing software or equipment approved by the United States Department of Defense;

(d) Incinerator or physical destruction; and

(e) Modify the information to make it unreadable, unusable or indecipherable through any means.

(K) Reporting of incidents involving personal information.

(1) A security breach in which personal information is disclosed to, or obtained by, an unauthorized person must be reported. Notification of the incident must be made in the most prompt and expedient manner after the incident has been discovered. Within 35 days, a letter notifying affected individuals of actual or suspected loss or disclosure of personal information must be sent describing the types of information lost and recommended actions to be taken to mitigate the potential misuse of their information.

(2) When it has been identified that a security breach has occurred in which personal information has been disclosed to, or obtained by, an unauthorized person, within three business days the point of contact shall notify the County Attorney or Commonwealth's Attorney, State Police, the Auditor of Public Accounts, the Attorney General and the Commissioner of the Department for Local Government and complete form COT-FOT2. The following shall be documented:

(a) Preliminary reporting and description of the incident;

(b) Response, including evidence gathered;

(c) Final assessment and corrective action taken; and

(d) Final reporting.

(3) Incident response procedures can be a reaction to security activities such as:

(a) Unauthorized access to personnel, data or resources;

(b) Denial of service attacks;

(c) Actual or anticipated widespread malware infections;

(d) Data breaches;

(e) Loss/theft of equipment;

(f) Significant disruption of services; and

(g) Significant level of unauthorized scanning activity to or from hosts on the network.

(L) Investigation. Reasonable efforts shall be made to investigate any security breaches in which personal information is disclosed to, or obtained by, an unauthorized person and appropriate corrective action shall be taken.

(M) Disclosure communications. All federal and state laws and policies for information disclosure to media or the public must be followed. In some circumstances, communication about an incident is necessary, such as contacting law enforcement. Employees should use discretion in disclosing information about an incident. Such information includes network information, type of incident, specific infection type (if applicable), number of assets affected, specific detail about applications affected, applications used to employ corrective action/investigate and the like. Within the parameters of the law, minimal disclosure regarding incidents is preferred to prevent unauthorized persons from acquiring sensitive information regarding the incident, security protocols and similar matters, in an effort to avoid additional disruption and financial loss.

SECTION VI. CODIFICATION. The provisions of Section I of this Ordinance shall be published as appropriate in the Franklin County Code of Ordinances as soon as practicable.

SECTION VII. SEVERABILITY CLAUSE. If any section, part of provision of this Ordinance is declared unconstitutional or invalid by a court of competent jurisdiction, then it is expressly provided and it is the intention of the Franklin County Fiscal Court in passing this Ordinance that its parts shall be severable and all other parts of this Ordinance shall not be affected thereby and they shall remain in full force and effect.

SECTION VIII. PUBLICATION AND EFFECTIVE DATE. This Ordinance shall take effect immediately upon its passage and publication according to law.

INTRODUCED AND GIVEN FIRST READING IN SUMMARY at a duly convened meeting of the Fiscal Court of Franklin County, Kentucky, held on the 18th day of December, 2025.

GIVEN SECOND READING AND APPROVED at a duly convened meeting of the Fiscal Court of Franklin County, Kentucky, held on the 7 day of January, 26 and of record in Fiscal Court Order Book 36, Page 527.

Michael Mueller
Franklin County Judge/Executive

ATTESTED TO:

Kim Cox
Fiscal Court Clerk

SUMMARY
This ordinance approves an amendment to Chapter 30, §30.170, §30.171, §30.172, §30.173, and §30.174, and §30.025 (A), (B), (C), (D), (E), (F), (G), (H), (I), (J), (K), (L) and (M) of the Administrative Code relating to Other County Policies