QUAINT OAK BANCORP, INC.
AND SUBSIDIARIES

CODE OF CONDUCT AND ETHICS

(as of May 13, 2026)

INTRODUCTION

Quaint Oak Bancorp, Inc. and its subsidiaries are committed to conducting business in a lawful, ethical, and responsible manner. Each Director, officer, and employee is personally responsible for acting with integrity, complying with applicable laws, rules, and regulations, and avoiding actual or perceived conflicts of interest. This Code of Conduct and Ethics (the "Code") has been adopted by the Board of Directors to provide standards of ethical conduct and to guide decisions and actions taken on behalf of Quaint Oak Bancorp, Inc. and its subsidiaries.

This Code outlines the broad principles of legal and ethical business conduct embraced by Quaint Oak Bancorp, Inc. and its subsidiaries. However, a written code cannot answer all questions raised in the context of business relationships. Therefore, this Code must be applied using common sense and good judgment. Issues with respect to conflicts, legality or ethics may not always be clear cut and officers and employees should consult with higher levels of management or the designated Compliance Officer. Directors should discuss the matter with the Compliance Officer or outside counsel.

CODE OF CONDUCT AND ETHICS – INDEX

ARTICLE I. ETHICAL PRINCIPLES AND CORPORATE VALUES 1

ARTICLE II. CONFLICTS OF INTEREST 1

A. Corporate Opportunities. 1

B. Loans Involving Employees. 2

C. Compensation and Gifts. 2

D. Business Gratuities. 4

E. Transactions with Insiders; Related Party Transactions. 4

ARTICLE III. CONFIDENTIAL INFORMATION 5

A. Confidential Information Regarding Customers and Others. 5

B. Permissible Dissemination of Confidential Information. 5

C. Confidential Information Regarding Current or Former Directors and Employees. 5

D. Company Resources; Proprietary Information. 5

ARTICLE IV. PERSONAL INVESTMENTS AND FINANCES 5

A. Insider Trading. 5

B. Personal Investments. 6

C. Purchase of Company Owned Property. 6

D. Loans. 7

ARTICLE V. BUSINESS CONDUCT 7

A. Business and Accounting Practices. 7

B. Political Contributions; Expenditures for Political Purposes 8

C. Information Security - Use of Company Owned Computers, Networks, Hardware and Software. 8

D. Outside Business Interests. 9

E. Management Interlocks. 9

ARTICLE VI. SPECIAL ETHICS OBLIGATIONS FOR EMPLOYEES WITH FINANCIAL REPORTING RESPONSIBILITIES 9

A. Standards of Ethical Conduct for Senior Financial Officers. 10

B. Waivers and Amendments. 10

C. Oversight by the Audit Committee. 10

ARTICLE VII. FRAUD AND ANTI-MONEY LAUNDERING COMPLIANCE 12
A. Prohibited Activities. 12
B. Customer Due Diligence and Recordkeeping. 12
C. Reporting Suspicious or Fraudulent Activity. 13
D. Confidentiality of Investigations and Reporting. 13
E. Cooperation with Regulatory Authorities. 13
F. Enforcement. 13
ARTICLE VIII. THIRD-PARTY VENDOR CONDUCT 14
A. Ethical Business Conduct. 14
B. Compliance with Laws and Regulations. 14
C. Confidentiality and Information Security. 14
D. Due Diligence and Risk Management. 15
E. Prohibited Conduct. 15
F. Reporting Concerns. 15
ARTICLE IX. CYBERSECURITY AND ACCEPTABLE USE 15
A. Acceptable Use of Company Systems. 16
B. Protection of Confidential Information. 16
C. Use of Personal Devices and Remote Access. 16
D. Cybersecurity Incident Reporting. 17
E. Monitoring and Privacy. 17
ARTICLE X. RECORDS RETENTION AND DOCUMENT INTEGRITY 17
A. Accurate Recordkeeping. 17
B. Retention and Preservation of Records. 18
C. Litigation Holds and Regulatory Inquiries. 18
D. Electronic Communications and Information. 18
ARTICLE XI. REGULATORY EXAMINATION COOPERATION 19
A. Duty to Cooperate. 19
B. Coordination of Regulatory Communications. 19
C. Preservation of Records. 19
D. Confidentiality. 20
E. Enforcement 20

ARTICLE XII. ARTIFICIAL INTELLIGENCE AND AUTOMATED SYSTEMS USE.. 20
A. Authorized Use of AI and Automated Systems. 20
B. Data Privacy and Confidentiality. 21
C. Accuracy, Validation, and Human Oversight. 21
D. Third-Party AI Systems. 21
E. Reporting and Incident Response. 22
ARTICLE XIII. REPORTING VIOLATIONS 22
ARTICLE XIV. WHISTLEBLOWER PROCEDURES 22
A. Reporting Illegal or Unethical Behavior 22
B. Accounting Complaints 22
C. Non-Retaliation 23
ARTICLE XV. CONCLUSION 23

ARTICLE I. ETHICAL PRINCIPLES AND CORPORATE VALUES

The nature of our business requires careful observance of applicable laws and regulations. High standards of conduct and personal integrity are essential for us to maintain the confidence of our shareholders, customers, employees, and the general public. In order to ensure that we and all of our Directors, officers and employees embrace and promote sound ethical business practices, we require that you agree to:

- Act with honesty and integrity, avoiding actual or apparent conflicts of interest in personal and professional relationships;

- Comply with rules and regulations of federal, state and local governments, and other appropriate regulatory agencies;

- Act in good faith, responsibly, and with due care, competence and diligence, without misrepresenting material facts or allowing one's independent judgment to be impaired;

- Provide information that is accurate, complete, objective, relevant, timely and understandable to ensure full, fair, accurate, timely, and understandable disclosure in reports and documents; and

- Promptly report to our President, Chief Executive Officer (CEO), Chief Financial Officer (CFO) or Compliance Officer or a member of the Audit Committee of our Board of Directors any conduct that you believe to be a violation of law or business ethics or of any provision of this Code, including any transaction or relationship that reasonably could be expected to give rise to a conflict of interest.

ARTICLE II. CONFLICTS OF INTEREST

A conflict of interest exists whenever you (or a member of your immediate family) has a personal interest in any entity or matter that may influence a decision or cloud your judgment in the discharge of your responsibilities to us. It is your duty to avoid situations from which you (or an immediate family member) might benefit personally, directly or indirectly, or that give the perception that you (or an immediate family member) is benefiting personally, from business decisions, use of our facilities or from relationships with our customers, vendors or contacts.

A. Corporate Opportunities.

If a business opportunity relating to our lines of business becomes available to or is made known to you, it must first be made available to Quaint Oak Bancorp, Inc., Quaint Oak Bank or our other subsidiaries, and we must have determined not to pursue such opportunity before being acted upon by you, by your immediate family or by any other Director, officer or employee.

B. Loans Involving Employees.

Employees are prohibited from participating in the process of making loans to companies in which the employee has a substantial interest as an owner, director, officer, or partner, or to companies in which a member of his or her immediate family has such an interest, or to a member of his or her immediate family. In such instances, the employee may assist in administrative intake only but must not participate in underwriting, approval, or decision-making related to the loan. Such interests must be disclosed, and such loans must be directed to another loan officer. Also see Section IV (D), below.

Employees should avoid any relationship that would cause a conflict of interest with their duties and responsibilities at Quaint Oak Bancorp, Inc. or its subsidiaries. Employees are expected to disclose any situations that may involve inappropriate or improper conflicts of interest affecting them personally or affecting other employees or those with whom we do business. Waivers of conflicts of interest involving executive officers require the approval of the Board of Directors or an appropriate committee.

To avoid conflicts of interest, Directors are expected to disclose to their fellow Directors any personal interest they may have in a transaction upon which the Board passes and to recuse themselves from participation in any decision in which there is a conflict or potential conflict between their personal interests and the interests of Quaint Oak Bancorp, Inc. or its subsidiaries.

C. Compensation and Gifts.

The Bank Bribery Act prohibits any Director or employee and any agent of Quaint Oak Bank or its subsidiaries or attorney representing us from offering or receiving anything of value where the item of value is offered with the intent of influencing the Director, officer or employee, agent or attorney or a business transaction. This law is broad and carries civil and criminal penalties, including fines and/or imprisonment. Gifts or awards given in recognition of your service or accomplishment in civic, charitable, educational, or religious organizations are not prohibited by this Code.

1. General Prohibitions: Except as provided below, you are prohibited from soliciting or receiving anything of value in any amount in connection with our business, including but not limited to money, goods, or services. This prohibition applies whether such was obtained as a gratuity/gift or as a “quid pro quo” exchange (something received or given as a reward for preferential action or service rendered by you). Additionally, this prohibition includes receiving compensation of any kind from any source for rendering services of a type that are performed or offered by us. A Director or employee may not do indirectly what he or she is prohibited from doing directly; for example, arrange to have a prohibited gift made to a member of his or her immediate family. Similarly, you may not give gifts, meals, or entertainment (including a quid pro quo exchange) which are intended to influence, or that might give the appearance of influencing, another Director, officer or employee or a business contact in a business decision. Any action by you perceived to compromise another's judgment is prohibited.

Example: An employee may not solicit or receive any sort of personal compensation in return for Quaint Oak Bank making a loan to a customer.

Example: A Director who is in a position, whether directly or indirectly, to sell goods or services to Quaint Oak Bank may not give gifts to the department responsible for making such purchasing decisions.

2. Permissible Gifts: Any Director, officer or employee may accept anything of value from customers only if it:

   a. Is valued at $200 or less, **AND**
   b. Is not intended to influence any decision by the Director, officer or employee;
   c. Is unsolicited;
   d. Is infrequent; and
   e. Is not a quid pro quo.

   Multiple gifts from the same source within a 12-month period must be aggregated for purposes of determining whether the $200 value threshold has been exceeded.

   Directors, officers and employees are prohibited from accepting cash or cash equivalent gifts including gift cards, prepaid debit cards, or negotiable instruments under any circumstances.

   Examples of Permissible Gifts: Gifts which are likely to meet these guidelines are: advertising or promotional materials such as pens, pencils, key rings, calendars and similar items valued under $200.

   Additionally, you may accept gifts from individuals who have both a personal relationship with you and a business relationship with us, for such commonly recognized events or occasions such as a promotion, wedding, birthday, retirement, or religious observance, if valued at less than $200.

Generally, there is no threat of a violation of the Bank Bribery Act if acceptance of a gift or benefit is based on an immediate family or personal relationship, which exists independent of any business with us or if the gift or benefit is made available to the general public under the same conditions on which it is made available to you.

If you are offered or receive something of value in excess of the above-stated amounts which you believe may be impermissible under this Code, you must disclose the matter to the Compliance Officer and seek a determination that the item of value may be accepted or must be returned. The reviewer will give due consideration to the criteria for permissible gifts and whether receipt poses a threat to our integrity.

D. Business Gratuities.

Payments for travel, lodging, meals and entertainment are normally permissible if they (i) are reasonable in amount; (ii) are expended in the course of a legitimate business meeting or an event intended to foster better business relations; (iii) would be paid by us as a business expense if not paid for by the outside source; and (iv) are unsolicited. Any travel or lodging paid for by an outside source must receive prior written approval from the employee's supervisor or the Compliance Officer.

If you are offered payments of the type which you believe may be impermissible, you must disclose the matter to the Compliance Officer and seek a determination that the offer may be accepted or must be rejected. The reviewer will give due consideration to the criteria for permissible payments and whether receipt poses a threat to our integrity.

Example: It is not a prohibited business gratuity to accept a vendor's offer to pay lodging and meals for an employee's attendance at a conference sponsored in whole or in part by the vendor so long as the employee's attendance has a business purpose.

E. Transactions with Insiders; Related Party Transactions.

From time to time we may purchase or lease real or personal property or goods or services from you, a member of your immediate family, or from business entities in which you or in which a member of your immediate family is an officer, director and/or controlling shareholder.

It is our policy that any transaction involving insiders must be conducted at arm's length and that any consideration paid or received by us in connection with such a transaction shall be on terms no less favorable than terms available to an unaffiliated third party under the same or similar circumstances. In accordance with Regulation O, the Director's or officer's interest in any such transactions requiring Board action shall be disclosed to the Board prior to any action being taken, and any such transactions not requiring Board approval shall be reported to the Board quarterly.

The Audit Committee must approve in advance all Related Party Transactions. For these purposes, a "Related Party Transaction" is any transaction, other than banking transactions in the normal course of business with no preferential terms and not involving more than the normal risk of collectability, between Quaint Oak Bancorp, Inc. or its subsidiaries and:

- any Director or executive officer;
- 5% or greater shareholder;
- any immediate family member of a Director, executive officer or 5% shareholder; or
- an entity in which a Director, executive officer, 5% shareholder or any immediate family member thereof, has a controlling or substantial ownership interest.

Any individual with a material interest in a Related Party Transaction must recuse themselves from discussion, evaluation, and approval of such transaction.

ARTICLE III. CONFIDENTIAL INFORMATION

A. Confidential Information Regarding Customers and Others.

You must take reasonable administrative, technical, and physical safeguards to protect the confidentiality of non-public information about us or our subsidiaries and our customers, shareholders and suppliers obtained or created in connection with your activities and to prevent the unauthorized disclosure of such information unless required by applicable law or regulation or legal or regulatory process.

B. Permissible Dissemination of Confidential Information.

Dissemination of confidential customer information among our affiliated entities, if any, is permissible. Notwithstanding the foregoing, all queries of a legal nature that involve confidential information relating to our customers must be directed to outside counsel.

C. Confidential Information Regarding Current or Former Directors and Employees.

All requests for information regarding current or former Directors or employees must be referred to our Compliance Officer. Our internal procedures and applicable laws limit the amount of information our Compliance Officer may provide.

D. Company Resources; Proprietary Information.

You are prohibited from selling, disclosing, or otherwise using our physical resources or proprietary information for personal benefit or for the benefit of any other party. The definition of our "physical resources or proprietary information" includes all of our intellectual property, including but not limited to any written materials, any computer or network-based information, data, any other types of information or data developed for us by an employee or a vendor, supplier or other contractor.

Example: Employees are prohibited from using our marketing research for a personal venture or disclosing proprietary information to a competitor.

ARTICLE IV. PERSONAL INVESTMENTS AND FINANCES

A. Insider Trading.

In the course of your duties, you may become privy to "insider information" within the meanings of state or federal laws. This means material, non-public information that might have an effect on our stock price if the information were publicly known. You should also be aware that the same prohibition against insider trading applies to trading in the stock of our customers, suppliers or any other company if you have inside information about them. Employees are strictly prohibited from providing inside information to other persons as this information might influence their trading activities or financial transactions. Employees must not disclose material non-public information through social media, messaging applications, or informal communications.

Examples of such "inside information" may include expansion plans, major management changes, future dividend rates, declaration of stock split or offerings of additional securities, current or future earnings projections, new contracts or projects, mergers, acquisitions or divestitures or other such material matters. It should be noted that either positive or negative information may be material.

Furthermore, information related to regulatory examinations, findings, inquiries or correspondence may be deemed to be material non-public information about Quaint Oak Bancorp, Inc. Accordingly, under the Quaint Oak Bancorp, Inc.'s Statement of Policy and Procedures Governing Trading in Shares of Quaint Oak Bancorp, Inc. ("Insider Trading Policy") and this Code, persons aware of this information should not trade in any securities of Quaint Oak Bancorp, Inc. while in possession of such information. Violations may subject you to civil or criminal penalties under the federal securities laws.

You are also prohibited from trading in put options or in short selling or in any other trade which would gain from a decrease in our stock price.

It is your responsibility to understand laws and policies that may apply to you. Further information on blackout periods, pre-clearance and other matters related to insider trading for Directors and executive officers are contained in the Insider Trading Policy.

B. Personal Investments.

Directors must disclose to the Chairman of the Board and employees must disclose to their direct supervisor when they know of any ownership or beneficial interest which they or members of their immediate families have with our customers or suppliers if they have responsibility for the account relationship. You and your immediate families are prohibited from investing in securities of customers or suppliers if you or they hold or share any responsibility for the account relationship, unless the securities are publicly traded and the purchase or sale is based upon information available to the general public, or unless approval is granted by a majority vote of the Board of Directors. In those instances where a personal investment in a given customer has been approved, you must avoid participation in any decisions concerning that customer.

Example: An employee who is the account officer for or deals with the loan account of ABC Company (a customer) may not invest personally in ABC Company without receiving prior approval of the Board of Directors. (See also Section IV (D) "Loans" below).

C. Purchase of Company Owned Property.

Purchase of company owned or subsidiary owned property (real or personal) by you or members of your immediate families requires the approval of the Board of Directors and must be at fair market value.

D. Loans.

Loans by us are available to Directors and executive officers on the same terms and conditions, including interest rates and collateral, as those prevailing for comparable loans with other customers. Loans are available to other employees consistent with the provisions of Regulation O ("Regulation O Loans"). Any loan to a Director, officer or other employee must not involve more than the normal risk of repayment or present other unfavorable features.

With certain exceptions, including loans by insured depository institutions which are subject to the restrictions of Section 22(h) of the Federal Reserve Act, the Securities Exchange Act of 1934, as amended (the "Exchange Act"), makes it unlawful for us, directly or indirectly, including through any subsidiary, to extend or maintain credit, arrange for the extension of credit or renew the extension of credit in the form of a personal loan to or for any of our Directors or executive officers.

Currently, Quaint Oak Bank does not make loans, other than those secured by Quaint Oak Bank deposit accounts, to any employees or their immediate family members which includes but is not limited to spouses, fiancés, significant others or domestic partners and those residing in the same household (whether related or not) unless the real estate loan is processed through Quaint Oak Mortgage and is sold into the secondary real estate market.

You are prohibited from lending personal funds to persons known to you as our customers, except if the customer is an immediate family member. You may not borrow from a customer unless the customer is a recognized lending institution.

ARTICLE V. BUSINESS CONDUCT

A. Business and Accounting Practices.

1. None of our funds or assets shall be used for unlawful purposes.

2. No unrecorded fund or asset shall be established or maintained for any purpose.

3. No false or misleading entries shall be made in our books and records for any purpose. All items of income or expense shall be appropriately recorded.

4. No payment by us shall be made with the intent or understanding that all or any part of such payment be used for any purpose other than that described in our books and records.

5. No payment on our behalf shall be approved without adequate supporting documentation or with the intention or understanding that all or any part of such payment is to be used for any purpose other than that described by the documents supporting the payment.

6. Compliance is required with generally accepted accounting principles and procedures and with established internal accounting controls and procedures.

7. We may require submission by Directors and employees of reports or statements in compliance with this section, at such time or from time to time and in such form as we may specify.

B. Political Contributions; Expenditures for Political Purposes.

1. None of our funds or assets are to be used to make any unlawful political contribution. For purposes of this section, the term "political contribution" includes not only the direct or indirect delivery of our cash or property to a political party, candidate, committee or organization but also includes: (a) the reimbursement by us to any Director, officer or employee or any other person, for a political contribution made or to be made by such Director, officer or employee or other person; or (b) the provision of services or the use of property or the making of a loan, to a political party, candidate, committee or organization by us, except in the ordinary course of our business and on customary commercial terms. Purchases of tickets to political dinners or other similar events or of advertisements in political publications are considered to be political contributions and are not reimbursable.

2. Neither we nor you acting on our behalf shall establish any program to solicit, collect or distribute political contributions from a Director, officer or employee.

3. You shall not be under any obligation of any kind to us or to any other Director, officer or employee, to utilize any of your compensation to make political contributions and no Director, officer or employee or any other person acting on our behalf, shall seek to create or enforce any such obligation.

Nothing contained in this section is intended to discourage you from active personal involvement in the political process, including the making of personal political contributions, or to otherwise limit the rights and obligations of Directors, officers or employees as responsible citizens. Directors, officers and employees engaging in personal political activity must do so on their own time and may not use company resources, premises, systems, or email addresses for political purposes. Notwithstanding the foregoing, this Code (i) requires that before you seek or accept a nomination or appointment to any public office, whether paid or unpaid, that you must obtain our non-objection and (ii) prohibits political campaigning, wearing and/or displaying political campaign slogans, distributing political literature, and/or soliciting campaign funds at or in the work place.

C. Information Security - Use of Company Owned Computers, Networks, Hardware and Software.

The unauthorized use or duplication of computer software owned by us is strictly prohibited. The use of computer software owned personally by employees on computer equipment owned by us is strictly prohibited. The use of personal devices to access company systems or confidential information must comply with company-approved security controls.

D. Outside Business Interests.

Prior approval must be obtained in situations where you or your immediate family members may profit from a relationship with a company or other entity with which you deal with in the course of your company duties.

E. Management Interlocks.

You should be aware of the various statutes and regulations either prohibiting or restricting dual service by you in the following areas:

1. Service as a director, officer or employee of any other commercial bank, banking association, trust company, savings bank, savings and loan association, or credit union;

2. Service in an organization primarily engaged in the issue, underwriting, public sale or distribution of stocks, bonds or other securities;

3. Service as an officer or director of a public utility or a registered public utility holding company or subsidiary; or

4. Service as a director, officer, partner, employee, appointee or representative of any obligor of securities for which our subsidiary with which he or she is affiliated is the indenture (corporate) trustee.

ARTICLE VI. SPECIAL ETHICS OBLIGATIONS FOR EMPLOYEES WITH FINANCIAL REPORTING RESPONSIBILITIES

As a public company, it is critical that Quaint Oak Bancorp, Inc.'s filings with the Securities and Exchange Commission ("SEC") be accurate and timely. Depending on your position with us, you may be called upon to provide information to assure that our public reports are complete, fair and understandable. We expect you to take this responsibility seriously and to provide prompt and accurate answers to inquiries related to our public disclosure requirements.

This Article VI serves as the Code of Ethics for Senior Financial Officers (this "Section 406 Code") which has been adopted by the Board of Directors of Quaint Oak Bancorp, Inc., in accordance with the requirements of Section 406 of the Sarbanes-Oxley Act of 2002 and the rules of the SEC promulgated thereunder.

This Section 406 Code applies to our Chief Executive Officer and Chief Financial Officer, and all other officers or employees who perform similar financial reporting or public disclosure functions (collectively, the "Senior Financial Officers"). In addition to being subject to all other provisions of the Code of Conduct and Ethics, Senior Financial Officers are subject to the standards set forth herein due to their critical roles in the preparation, review, certification, and oversight of our financial statements and disclosures filed with, or submitted to, the SEC and other regulatory authorities.

A. Standards of Ethical Conduct for Senior Financial Officers.

Because of this special role, our Senior Financial Officers are bound by the following standards, and by signing the Annual Certification for Senior Financial Officers attached to this Code, each agrees that he or she will:

- Act with honesty and integrity, avoiding actual or apparent conflicts of interest in personal and professional relationships;

- Provide information that is complete, objective, relevant, timely and understandable to ensure full, fair, accurate, timely, and understandable disclosure in reports and documents that we file with, or submit to, government agencies and in other public communications made by us;

- Comply with applicable rules and regulations of federal, state and local governments, and other appropriate regulatory agencies;

- Act in good faith, responsibly, and with due care, competence and diligence, without misrepresenting material facts or allowing one's independent judgment to be impaired; and

- Promptly report to the Audit Committee of our Board of Directors any conduct that the individual believes to be a violation of law or business ethics or of any provision of the Code of Conduct, including any transaction or relationship that reasonably could be expected to give rise to a conflict of interest.

Violations of these standards, including failures to report potential violations by others, are a serious matter that may result in disciplinary action, including termination of employment, and may also subject the individual to civil or criminal penalties under applicable law.. If you believe that a violation of these standards has occurred, you should contact the Audit Committee of the Board of Directors.

B. Waivers and Amendments.

Any waiver of this Section 406 Code for Senior Financial Officers may be made only by the Board of Directors or a duly authorized committee thereof and will be promptly disclosed to shareholders as required by applicable law and SEC regulations, including pursuant to Form 8-K or such other disclosure mechanism as may be permitted under SEC rules, in each case within the period prescribed by applicable rules and regulations. The Compliance Officer shall retain records relating to any such amendment or waiver in accordance with applicable legal and regulatory record retention requirements.

C. Oversight by the Audit Committee.

The Audit Committee of the Board of Directors shall be responsible for the oversight and administration of this Section 406 Code of Ethics for Senior Financial Officers.

In carrying out its responsibilities under this Section 406 Code, the Audit Committee shall:

- Monitor compliance by Senior Financial Officers with the provisions of this Section 406 Code;
- Review any reported violations of this Section 406 Code involving Senior Financial Officers;
- Oversee the investigation of any matters relating to alleged misconduct or ethical concerns pertaining to financial reporting, accounting practices, internal controls, or public disclosures;
- Determine, or recommend to the Board of Directors, as appropriate, disciplinary or remedial action in response to violations; and
- Review and approve any requests for waivers or amendments to the provisions of this Section 406 Code applicable to Senior Financial Officers.

The Audit Committee may delegate administrative responsibilities under this Section 406 Code to our Compliance Officer or other appropriate personnel; provided, however, that any waiver of the provisions of this Section 406 Code for a Senior Financial Officer shall be approved by the Board of Directors or a duly authorized committee thereof in accordance with applicable law and SEC regulations.

Annual Certification. All Senior Financial Officers shall, on an annual basis, certify in writing to the Compliance Officer that:

- They have reviewed and understand the provisions of this Section 406 Code of Ethics for Senior Financial Officers;
- They have complied with all applicable requirements set forth in this Section 406 Code during the preceding fiscal year;
- They are not aware of any known or suspected material violations of this Section 406 Code that have not been previously disclosed to the Audit Committee, the Compliance Officer, or other appropriate reporting authority; and
- They have promptly reported any known or suspected violations of applicable laws, rules, regulations, internal controls, or ethical standards relating to financial reporting or public disclosures in accordance with Quaint Oak Bancorp, Inc.'s reporting procedures.

Such Annual Certifications shall be maintained by the Compliance Officer in accordance with our applicable document retention policies and shall be made available to the Audit Committee upon request.

ARTICLE VII. FRAUD AND ANTI-MONEY LAUNDERING COMPLIANCE

Quaint Oak Bancorp, Inc. and its subsidiaries are committed to maintaining an effective system of internal controls designed to prevent, detect, and report fraud, money laundering, terrorist financing, and other financial crimes in accordance with applicable federal and state laws and regulations, including the Bank Secrecy Act ("BSA"), the USA PATRIOT Act, and related regulatory requirements. All Directors, officers, and employees are required to conduct business in a manner that supports our compliance with applicable anti-money laundering ("AML") and financial crimes prevention laws, rules, and regulations.

A. Prohibited Activities.

Directors, officers, and employees shall not knowingly:

- Engage in or facilitate fraudulent, deceptive, or dishonest conduct affecting Quaint Oak Bancorp, Inc. and its subsidiaries, our customers, vendors, or other third parties;
- Participate in or assist in money laundering, terrorist financing, or other financial crimes;
- Structure or assist in structuring transactions for the purpose of evading regulatory reporting requirements, including Currency Transaction Reports ("CTR") or Suspicious Activity Reports ("SAR");
- Falsify or omit material information in any company record, transaction documentation, or customer identification data; or
- Conduct transactions on behalf of customers or third parties in a manner designed to conceal the true source, ownership, control, or purpose of funds.

B. Customer Due Diligence and Recordkeeping.

Employees are required to follow all policies, procedures, and controls relating to:

- Customer identification and verification;
- Customer due diligence ("CDD") and enhanced due diligence ("EDD");
- Monitoring of customer transactions;
- Identification of suspicious or unusual activity; and
- Maintenance of accurate and complete records relating to customer accounts and transactions.

Employees must not knowingly open, maintain, or service any account that is established using false or misleading information or documentation.

C. Reporting Suspicious or Fraudulent Activity.

Each Director, officer, and employee has an affirmative obligation to promptly report any known or suspected: fraudulent activity; suspicious transactions; money laundering or structuring activity; attempts to bypass customer identification or verification procedures; or other potential violations of applicable financial crimes laws or internal controls.

All such reports must be made in accordance with our established reporting procedures, including escalation to the Compliance Officer, AML Officer, or other designated reporting authority.

Employees must not independently investigate suspected suspicious activity unless authorized to do so by appropriate personnel.

D. Confidentiality of Investigations and Reporting.

Directors, officers, and employees are strictly prohibited from disclosing:

- The existence or filing of a SAR;
- Information relating to an internal fraud or AML investigation; or
- Any inquiry or review conducted by regulatory or law enforcement authorities.

Unauthorized disclosure of such information may violate applicable law and policy and may result in disciplinary action.

E. Cooperation with Regulatory Authorities.

Quaint Oak Bancorp, Inc. and its subsidiaries shall cooperate fully with all lawful requests from regulatory and law enforcement authorities relating to fraud prevention, anti-money laundering compliance, or financial crimes investigations.

Directors, officers, and employees must promptly notify the Compliance Officer or Internal Corporate Counsel of any regulatory or law enforcement inquiries relating to Quaint Oak Bancorp, Inc., its subsidiaries or our customers and must not respond to such inquiries without authorization from the Compliance Officer or Internal Corporate Counsel.

F. Enforcement.

Failure to comply with applicable fraud prevention or anti-money laundering laws, regulations, or company policies may result in disciplinary action, up to and including termination of employment or service, and may subject the individual to civil or criminal liability.

ARTICLE VIII. THIRD-PARTY VENDOR CONDUCT

Quaint Oak Bancorp, Inc. and its subsidiaries rely on third-party vendors, service providers, consultants, contractors, and other business partners to support various aspects of our operations. Quaint Oak Bancorp, Inc. and its subsidiaries are committed to conducting business with vendors who demonstrate integrity, professionalism, and adherence to applicable legal and regulatory requirements.

Directors, officers, and employees are responsible for ensuring that the selection, engagement, and oversight of vendors are conducted in a manner that promotes ethical conduct, transparency, and compliance with applicable laws and our policies.

A. Ethical Business Conduct.

Employees involved in the procurement, selection, or management of vendors shall:

- Conduct vendor selection processes in a fair, objective, and transparent manner;
- Avoid actual or apparent conflicts of interest in vendor relationships;
- Ensure that all vendor engagements are based on legitimate business needs;
- Refrain from accepting gifts, favors, or other items of value from vendors that could improperly influence business decisions; and
- Comply with our policies relating to vendor management, purchasing, and approval authorities.

B. Compliance with Laws and Regulations.

Employees must take reasonable steps to ensure that vendors:

- Comply with applicable federal, state, and local laws and regulatory requirements;
- Maintain appropriate licenses, permits, and certifications, where applicable;
- Conduct their business activities in a lawful and ethical manner; and
- Support our obligations relating to consumer protection, anti-money laundering, data privacy, and information security.

Quaint Oak Bancorp, Inc. and its subsidiaries will not knowingly engage vendors who participate in unlawful, fraudulent, or unethical practices.

C. Confidentiality and Information Security.

Employees must ensure that appropriate contractual provisions addressing confidentiality, data protection, and information security are included in vendor agreements. Vendors who are provided access to confidential or non-public company information must be required to:

- Maintain the confidentiality of such information;
- Use company information solely for authorized business purposes; and

- Implement appropriate administrative, technical, and physical safeguards to prevent unauthorized access, disclosure, or misuse.

D. Due Diligence and Risk Management.

Vendor relationships must be periodically reviewed in accordance with our policies to ensure ongoing compliance with contractual obligations and regulatory expectations. Prior to engaging a vendor, employees must follow applicable company procedures for:

- Vendor due diligence and risk assessment;
- Review of financial condition and operational capabilities;
- Evaluation of legal, compliance, and reputational risks; and
- Approval by appropriate supervisors or oversight committees, as required.

E. Prohibited Conduct.

Directors, officers, and employees shall not:

- Circumvent established vendor selection or approval procedures;
- Enter into side agreements or undisclosed arrangements with vendors;
- Direct vendors to engage in activities that violate applicable laws or our policies; or
- Use vendors to perform activities that are prohibited to our employees under applicable law or internal policies.

F. Reporting Concerns.

Employees who become aware of any unethical, unlawful, or otherwise inappropriate conduct by a vendor must promptly report such conduct in accordance with our reporting procedures.

ARTICLE IX. CYBERSECURITY AND ACCEPTABLE USE

Quaint Oak Bancorp, Inc. and its subsidiaries are committed to protecting the confidentiality, integrity, and availability of its information systems, customer information, and proprietary data. All Directors, officers, and employees share responsibility for safeguarding our information assets and for ensuring that company-owned technology systems are used in a secure, responsible, and lawful manner.

Company information systems include, but are not limited to:

- Computer hardware and software
- Electronic mail systems
- Internet and network access
- Mobile devices
- Databases and digital storage media
- Cloud-based systems
- Telecommunications systems

- Any other technology resource owned, leased, or operated by Quaint Oak Bancorp, Inc. or its subsidiaries

A. Acceptable Use of Company Systems.

Directors, officers, and employees shall use company information systems and technology resources primarily for legitimate business purposes and in accordance with our applicable policies and procedures. Users of company systems are prohibited from:

- Engaging in unauthorized access to company systems, data, or networks;
- Installing unauthorized software, applications, or hardware;
- Accessing, storing, or transmitting illegal, fraudulent, or inappropriate materials;
- Disabling or attempting to circumvent security, monitoring, or access-control systems;
- Using company systems for personal financial gain or non-business commercial activity; or
- Using company technology resources in any manner that could compromise system security or operational integrity.

Limited incidental personal use of Company-provided systems may be permitted, provided that such use does not interfere with business operations, violate our policies, or compromise the security or integrity of company systems or information.

B. Protection of Confidential Information.

Directors, officers, and employees are required to:

- Protect the confidentiality of non-public company and customer information;
- Use company information solely for authorized business purposes;
- Safeguard passwords, authentication credentials, and access devices;
- Log off or secure devices when unattended; and
- Ensure that confidential information is not disclosed to unauthorized persons.

Confidential or sensitive information must not be transmitted through unsecured communication methods or stored on unauthorized devices or external storage media.

C. Use of Personal Devices and Remote Access.

The use of personal devices to access company information systems or confidential information must comply with company-approved security controls, including any applicable requirements relating to device management, encryption, authentication, and monitoring. Remote access to company systems must be authorized and conducted only through secure methods approved by our Information Technology or Information Security personnel.

D. Cybersecurity Incident Reporting.

Directors, officers, and employees must promptly report any known or suspected:

- Unauthorized access to company systems or information;
- Loss or theft of company devices or data;
- Malware infections or system vulnerabilities;
- Phishing or social engineering attempts; or
- Other cybersecurity incidents or suspected information-security breaches.

Reports must be made immediately to our Information Technology Department, Compliance Officer, or other designated reporting authority in accordance with Company incident-response procedures.

Employees must not attempt to investigate or remediate suspected cybersecurity incidents unless authorized to do so by appropriate company personnel.

E. Monitoring and Privacy.

We reserve the right, to the fullest extent permitted by applicable law, to monitor, access, review, and disclose all data, communications, and activities conducted through or stored on our information systems for legitimate business purposes, including ensuring compliance with our policies, regulatory requirements, and applicable law.

You should have no expectation of privacy with respect to information created, transmitted, received, or stored on our information systems.

ARTICLE X. RECORDS RETENTION AND DOCUMENT INTEGRITY

Quaint Oak Bancorp, Inc. and its subsidiaries are committed to maintaining accurate, complete, and reliable records in accordance with applicable legal, regulatory, accounting, and operational requirements. Proper records retention and document integrity are essential to our ability to meet its legal obligations, support effective internal controls, and demonstrate compliance with applicable laws and regulations. All Directors, officers, and employees are responsible for the creation, maintenance, retention, and disposal of our records in accordance with our approved record retention policies and applicable regulatory requirements.

A. Accurate Recordkeeping.

All of our books, records, accounts, reports, and financial statements must be:

- Prepared accurately and in a timely manner;
- Maintained in reasonable detail;
- Supported by appropriate documentation; and
- Reflective of actual transactions and events.

No undisclosed or unrecorded fund, account, asset, or liability shall be established or maintained for any purpose. Directors, officers, and employees shall not:

- Make false, misleading, or incomplete entries in company records;
- Conceal or misrepresent the true nature of any transaction; or
- Alter or manipulate information in any company document in a manner that misstates financial, operational, or compliance-related information.

B. Retention and Preservation of Records.

Directors, officers, and employees shall comply with all of our applicable policies relating to:

- Retention of business records in electronic or physical form;
- Secure storage of confidential or sensitive information;
- Protection against unauthorized access, destruction, or modification; and
- Timely and appropriate disposal of records in accordance with approved retention schedules.

Records must not be destroyed, modified, or otherwise disposed of in a manner that violates applicable legal or regulatory requirements or conflicts with our document retention policies.

C. Litigation Holds and Regulatory Inquiries.

Upon receipt of a notice of litigation, audit, examination, investigation, or regulatory inquiry, all applicable records, regardless of format, must be preserved in accordance with any litigation hold or document preservation directive issued by our Compliance Officer, Legal Department, or other authorized personnel. Directors, officers, and employees are strictly prohibited from:

- Destroying, altering, or concealing any document or record that may be relevant to a pending or anticipated investigation or legal proceeding; or
- Taking any action intended to impede, obstruct, or influence an internal or external audit, examination, or investigation.

D. Electronic Communications and Information.

Electronic records, including emails, messages, and other digital communications created or transmitted using our systems, constitute our records and may be subject to regulatory review, legal discovery, or internal audit. Employees must ensure that electronic communications relating to company business are:

- Retained in accordance with our policies;
- Stored on authorized corporate systems; and
- Not deleted or altered in violation of retention schedules or preservation directives.

ARTICLE XI. REGULATORY EXAMINATION COOPERATION

Quaint Oak Bancorp, Inc. and its subsidiaries are subject to examination, supervision, and regulation by various federal and state regulatory agencies, including but not limited to the Federal Deposit Insurance Corporation ("FDIC"), the Federal Reserve, the Securities and Exchange Commission ("SEC"), and the Pennsylvania Department of Banking and Securities.

All Directors, officers, and employees are required to cooperate fully with authorized regulatory, supervisory, and governmental authorities in connection with any examination, audit, inspection, inquiry, or investigation relating to our business, operations, financial reporting, internal controls, compliance programs, or other regulatory obligations.

A. Duty to Cooperate.

Directors, officers, and employees shall:

- Provide complete, accurate, and timely information in response to lawful requests from regulatory authorities;
- Participate in meetings, interviews, or reviews conducted by regulatory agencies as required;
- Produce documents, records, or data requested by authorized company personnel in connection with regulatory examinations or inquiries; and
- Refrain from making false, misleading, or incomplete statements to internal auditors, external auditors, or regulatory representatives.

B. Coordination of Regulatory Communications.

All communications with regulatory agencies concerning our operations, policies, records, or practices must be conducted through authorized personnel, including the Compliance Officer, Legal Department, or other designated members of senior management. Directors, officers, and employees must:

- Promptly notify the Compliance Officer or your supervisor of any regulatory inquiry or request for information;
- Refrain from responding directly to regulatory inquiries unless authorized to do so; and
- Escalate any requests for interviews, documents, or records in accordance with Company procedures.

C. Preservation of Records.

Upon notification of a pending or ongoing regulatory examination, investigation, or supervisory inquiry, all relevant records—whether in electronic or physical form—must be preserved in accordance with our records retention policies and any applicable document preservation or litigation hold directives. Directors, officers, and employees are strictly prohibited from:

- Destroying, altering, concealing, or falsifying any document or record relevant to a regulatory examination or inquiry; or
- Taking any action intended to impede, obstruct, or improperly influence the outcome of a regulatory review or supervisory process.

D. Confidentiality.

Information relating to regulatory examinations, findings, inquiries, or correspondence is considered "confidential supervisory information" and must not be disclosed to outside sources except as required by law. The regulations prohibit the disclosure of such confidential supervisory information, without the banking regulators' prior written consent, to anyone other than our Directors, officers or employees of Quaint Oak Bank who already have knowledge of the information, or certain representatives of Quaint Oak Bank, such as legal counsel or auditors.

E. Enforcement

Failure to handle confidential supervisory information in compliance with the regulations is a violation of those regulations and could subject you to dismissal from Quaint Oak Bank or supervisory action, including the imposition of civil money penalties, or in some instances, criminal penalties.

ARTICLE XII. ARTIFICIAL INTELLIGENCE AND AUTOMATED SYSTEMS USE

Quaint Oak Bancorp, Inc. and its subsidiaries may utilize various forms of artificial intelligence (commonly referred to as "AI"), automated decision-making tools, and data-driven technologies to support business operations, internal processes, customer interactions, and risk-management activities. The use of such technologies must be conducted in a lawful, ethical, transparent, and secure manner consistent with our obligations under applicable laws, regulations, and internal policies.

All Directors, officers, and employees are responsible for ensuring that any use of AI systems or automated technologies in connection with our operations is appropriate, authorized, and compliant with our established governance frameworks relating to information security, data privacy, model risk management, and operational risk management.

A. Authorized Use of AI and Automated Systems.

Directors, officers, and employees shall use only AI tools, automated systems, or data-processing technologies that have been approved by us for legitimate business purposes. Employees are prohibited from:

- Using unauthorized third-party AI applications or tools to process our corporate, customer, or proprietary information;
- Entering confidential, non-public, or personal customer data into publicly accessible AI platforms;

- Utilizing automated technologies to make decisions or recommendations without appropriate human oversight where required by our policies; or
- Deploying internally developed or third-party automated systems without appropriate review and approval by our Information Technology, Compliance, or Risk Management personnel.

B. Data Privacy and Confidentiality.

Any use of AI or automated systems must comply with our applicable policies, contractual obligations, and legal requirements relating to:

- Protection of non-public personal information ("NPI");
- Confidential supervisory information;
- Customer due diligence data;
- Financial reporting information; and
- Proprietary corporate data or intellectual property.

Employees must not upload or disclose confidential or sensitive corporate or customer information into any AI-based application or service that has not been specifically approved for secure enterprise use.

C. Accuracy, Validation, and Human Oversight.

Outputs generated by AI or automated decision-making tools must be reviewed for accuracy, reasonableness, and consistency prior to use in any customer-facing, financial reporting, compliance, or operational decision-making process. Employees shall not rely exclusively on automated outputs or system-generated recommendations in situations involving:

- Credit underwriting or lending decisions;
- Customer due diligence or risk scoring;
- Financial reporting or regulatory disclosures;
- Fraud detection or compliance risk assessments; or
- Any activity requiring professional judgment or regulatory compliance determinations.

Appropriate human oversight must be exercised to ensure that the use of AI-assisted outputs does not result in material errors, regulatory violations, or unintended risk exposures.

D. Third-Party AI Systems.

Any third-party vendor providing AI-enabled services must be subject to appropriate due diligence, contractual protections, and ongoing monitoring in accordance with our Third-Party Vendor Conduct policies. Employees must ensure that any AI-enabled Vendor solutions are evaluated for:

- Data security and confidentiality protections;
- Compliance with applicable regulatory requirements;

- Model transparency or explainability, where appropriate; and
- Accuracy and reliability in performing intended business functions.

E. Reporting and Incident Response.

Directors, officers, and employees must promptly report any known or suspected:

- Unauthorized use of AI tools;
- Data privacy or confidentiality breaches involving automated systems;
- System errors resulting in inaccurate customer or financial information;
- Security vulnerabilities associated with AI-enabled technologies; or
- Potential regulatory or compliance risks arising from automated decision-making processes.

Reports must be made in accordance with our established incident-response or reporting procedures.

ARTICLE XIII. REPORTING VIOLATIONS

The procedures for handling concerns and complaints regarding questionable accounting or auditing matters are set forth below under Article VIII, "Whistleblower Procedures."

Anyone who seeks advice, raises a concern or reports misconduct or a violation of this Code is following the requirements of this Code and the desires of our Board of Directors. We encourage such action. Retaliation against anyone who makes a good faith report of misconduct is illegal and will not be tolerated.

ARTICLE XIV. WHISTLEBLOWER PROCEDURES

A. Reporting Illegal or Unethical Behavior

If you suspect or know of violations of this Code or illegal or unethical business or workplace conduct by employees, officers or Directors then you have an obligation to contact your supervisor or superiors. If the individuals to whom such information is conveyed are not responsive, or if there is a reason to believe that reporting to such individuals is inappropriate in particular cases, then you should contact the President, CEO, or CFO. Such communications will be kept confidential to the extent feasible. If you are still not satisfied with the response, then you may contact the Audit Committee of the Board of Directors, Attention Andrew E. DiPiero, Jr., at 501 Knowles Avenue, Southampton, Pennsylvania 18966. If concerns or complaints require confidentiality, then this confidentiality will be protected to the extent feasible, subject to applicable law.

B. Accounting Complaints

Our policy is to comply with all applicable financial reporting and accounting regulations. If any Director, officer or employee has unresolved concerns or complaints regarding questionable

accounting or auditing matters, then you are encouraged to submit those concerns or complaints (anonymously, confidentially or otherwise) to the Audit Committee. Subject to its legal duties, the Audit Committee and the Board will treat such submissions confidentially. Such submissions may be directed to the attention of the Audit Committee of the Board of Directors, 501 Knowles Ave, Southampton, Pennsylvania 18966.

C. Non-Retaliation

We prohibit retaliation of any kind against individuals who have made good faith reports or complaints of violations of this Code or other known or suspected illegal or unethical conduct. Retaliation against any individual who reports a concern in good faith is strictly prohibited and may result in disciplinary action up to and including termination.

ARTICLE XV. CONCLUSION

We conduct ourselves and our business dealings so as to comply with all applicable laws and regulations. Where the requirements of such laws and regulations are unclear, the advice of the Compliance Officer or outside counsel must be sought to secure interpretation and to ensure compliance. You must understand our internal policies and procedures and the legal and regulatory framework within which we operate and must take those steps necessary to ensure that any persons working with or under your supervision understand them. You are urged to reread this Code from time to time to refresh your recollection of the statutory and regulatory matters and the policies outlined herein.

This Code may be amended or modified by our Board of Directors. Waivers of this Code may only be granted by the Board of Directors or a committee of the Board with specific delegated authority. Waivers will be disclosed to shareholders as required by the Exchange Act and the rules thereunder.

CERTIFICATE OF COMPLIANCE

I have reviewed and read the Code of Conduct and Ethics for Quaint Oak Bancorp, Inc. and its subsidiaries as adopted by the Board of Directors on May 13, 2026.

I hereby certify that I am complying with all provisions of the Code and that I am not aware of any violations of the Code, except as noted below:

_____
_____
_____

I understand that the Code requires that if I become aware of any violations of the Code, I must report them.

I have read and understand the Code and agree to comply with it at all times and in connection with the purchase and sale of Quaint Oak Bancorp, Inc. stock.

I also understand that violations of the Code can result in sanctions, including discipline, suspension, discharge, and referral for criminal prosecution or civil action.

Date: _____

Signature: _____

Name (printed or typed): _____

PLEASE SIGN, DATE, AND RETURN TO:
Rachel A. Clarkson
Compliance Officer
Quaint Oak Bank

SECTION 406 CODE FOR SENIOR FINANCIAL OFFICERS

ANNUAL CERTIFICATION

Pursuant to the Code of Ethics for Senior Financial Officers (the "Section 406 Code"), adopted in accordance with Section 406 of the Sarbanes-Oxley Act of 2002 and the rules of the Securities and Exchange Commission, I hereby certify the following:

1. I have received, reviewed, and understand the provisions of the Section 406 Code for Senior Financial Officers.

2. I have complied with the requirements and standards set forth in the Section 406 Code during the preceding fiscal year.

3. I am not aware of any known or suspected material violations of the Section 406 Code that have not been previously disclosed to the Audit Committee of the Board of Directors, the Compliance Officer, or other appropriate reporting authority.

4. I have promptly reported any known or suspected violations of applicable laws, rules, regulations, internal accounting controls, financial reporting obligations, or ethical standards relating to the preparation, review, or disclosure of Quaint Oak Bancorp, Inc.'s financial statements or public filings in accordance with Quaint Oak Bancorp, Inc.'s reporting procedures.

5. I understand that compliance with the Section 406 Code is a condition of my continued service with Quaint Oak Bancorp, Inc. and that failure to comply with its provisions may result in disciplinary action, up to and including termination of employment or service, and may also subject me to civil or criminal liability under applicable law.

6. I agree to promptly inform the Compliance Officer of any future actual or apparent conflicts of interest or other circumstances that may give rise to a violation of the Section 406 Code.

Disclosure of exceptions (if any). Please describe below any known or suspected violations, conflicts of interest, or other matters that may require disclosure pursuant to the Section 406 Code:

_____

_____

Date: _____

Signature: _____

Name (printed or typed): _____

PLEASE SIGN, DATE, AND RETURN TO:
Rachel A. Clarkson
Compliance Officer
Quaint Oak Bank