

OHIO ATHLETIC COMMISSION

Confidential Personal Information Policy

1.0 Definitions

(A) "Access" as a noun means an opportunity to copy, view, or otherwise perceive whereas "access" as a verb means to copy, view, or otherwise perceive.

(B) "Acquisition of a new computer system" means the purchase of a "computer system," as defined in this rule, that is not a computer system currently in place nor one for which the acquisition process has been initiated as of the effective date of the commission rule addressing requirements in section 1347.15 of the Revised Code.

(C) "Computer system" means a "system," as defined by section 1347.01 of the Revised Code, that stores, maintains, or retrieves personal information using electronic data processing equipment.

(D) "Confidential personal information" has the meaning as defined by division (A)(1) of section 1347.15 of the Revised Code and identified by rules promulgated by the commission in accordance with division (B)(3) of section 1347.15 of the Revised Code that reference the federal or state statutes or administrative rules that make personal information maintained by the commission confidential.

(E) "Employee of the commission" means each employee of the Ohio Athletic Commission as well as each member of the Ohio Athletic Commission appointed to the commission pursuant to section 3773.33 of the Ohio Revised Code.

(F) "Incidental contact" means contact with the information that is secondary or tangential to the primary purpose of the activity that resulted in the contact.

(G) "Individual" means natural person or the natural person's authorized representative, legal counsel, legal custodian, or legal guardian.

(H) "Information owner" means the individual appointed in accordance with division (A) of section 1347.05 of the Revised Code to be directly responsible for a system.

(I) "Person" means natural person.

(J) "Personal information" has the same meaning as defined in division (E) of section 1347.01 of the Revised Code.

(K) "Personal information system" means a "system" that "maintains" "personal information" as those terms are defined in section 1347.01 of the Revised Code. "System" includes manual and computer systems.

(L) "Research" means a methodical investigation into a subject.

(M) "Routine" means common place, regular, habitual, or ordinary.

(N) "Routine information that is maintained for the purpose of internal office administration, the use of which would not adversely affect a person" as that phrase is used in division (F) of section 1347.01 of the Revised Code means personal information relating to the commission's employees that is maintained by the commission for administrative and human resource purposes.

(O) "System" has the same meaning as defined by division (F) of section 1347.01 of the Revised Code.

(P) "Upgrade" means a substantial redesign of an existing system for the purpose of providing a substantial amount of new application functionality, or application modifications that would involve substantial administrative or fiscal resources to implement, but would not include maintenance, minor updates and patches, or modifications that entail a limited addition of functionality due to changes in business or legal requirements.

2.0 Personal information systems

(A) The executive director of the commission shall be directly responsible for the personal information system maintained by the commission.

(B) The commission shall discipline any employee who initiates or otherwise contributes to any disciplinary or other punitive action taken against another individual who brings to the attention of appropriate authorities, the press, or a member of the public, any evidence of unauthorized use of any material contained in the personal information system.

(C) The commission shall maintain its personal information system with the accuracy, relevance, timeliness, and completeness necessary to assure fairness in any determination made by the commission that is based on information contained in the system.

(D) The commission shall investigate, upon request, the accuracy, relevance, timeliness, and completeness of the personal information which is disputed by the subject of a record contained in its personal information system and report its findings to the disputant within thirty days after receipt of the request.

(E) The commission shall not place personal information into an interconnected or combined system unless said system contributes to the efficiency of other agencies or organizations authorized by law to use the system.

(F) The commission shall not use any personal information placed into an interconnected or combined system by another state or local commission or an organization unless the personal information is necessary and relevant to the performance of a lawful function of the commission.

3.0 Procedures for accessing personal information

(A) Personal information systems of the commission are managed on a "need-to-know" basis whereby the information owner determines the level of access required for an employee of the commission to fulfill his or her job duties. The determination of access to confidential personal information shall be approved by the employee's supervisor and the information owner prior to providing the employee with access to confidential personal information within a personal

information system. The commission shall establish procedures for determining a revision to an employee's access to confidential personal information upon a change to that employee's job duties including, but not limited to, transfer or termination. Whenever an employee's job duties no longer require access to confidential personal information in a personal information system, the employee's access to confidential personal information shall be removed.

(B) Upon the signed written request of any individual for a list of confidential personal information about the individual maintained by the commission, the commission shall do all of the following:

- (1) Verify the identity of the individual by a method that provides safeguards commensurate with the risk associated with the confidential personal information;
- (2) Provide to the individual the list of confidential personal information that does not relate to an investigation about the individual or is otherwise not excluded from the scope of Chapter 1347. of the Revised Code; and
- (3) If all information relates to an investigation about that individual, inform the individual that the commission has no confidential personal information about the individual that is responsive to the individual's request.

(C) Upon discovery or notification that confidential personal information of a person has been accessed by an employee for an invalid reason, the commission shall notify the person whose information was invalidly accessed as soon as practical and to the extent known at the time. However, the commission shall delay notification for a period of time necessary to ensure that the notification would neither delay or impede an investigation of the circumstances and involvement of an employee surrounding the invalid access, nor jeopardize homeland or national security. Additionally, the commission may delay the notification consistent with any measures necessary to determine the scope of the invalid access, including which individuals' confidential personal information invalidly was accessed, and to restore the reasonable integrity of the system. Once the commission determines that notification would not delay or impede an investigation, the commission shall disclose the access to confidential personal information made for an invalid reason to the person. Notification provided by the commission shall inform the person of the type of confidential personal information accessed and the date(s) of the invalid access, and may be made by any method reasonably designed to accurately inform the person of the invalid access, including written, electronic, or telephone notice.

(D) The executive director shall designate an employee of the commission to serve as the data privacy point of contact. The data privacy point of contact shall work with the chief privacy officer within the office of information technology to assist the commission with both the implementation of privacy protections for the confidential personal information that the commission maintains and compliance with section 1347.15 of the Revised Code and the rules adopted pursuant to the authority provided by that chapter.

(E) The executive director shall designate an employee of the commission to serve as the data privacy point of contact who shall timely complete the privacy impact assessment form developed by the office of information technology.

4.0 Valid reasons for accessing confidential personal information

(A) Pursuant to the requirements of division (B)(2) of section 1347.15 of the Revised Code, this policy contains a list of valid reasons, directly related to the commission's exercise of its powers or duties, for which only employees of the commission may access confidential personal information regardless of whether the personal information system is a manual system or computer system.

(B) Any of the following functions normally performed by the commission constitute valid reasons for authorized employees of the commission to access confidential personal information:

- (1) Responding to a public records request;
- (2) Responding to a request from an individual for the list of confidential personal information the commission maintains on that individual;
- (3) Administering a provision of the United States constitution or Ohio constitution directly applicable to the operations of the commission;
- (4) Administering a provision of Chapter 3773. of the Revised Code;
- (5) Administering a provision of agency 3773 of the Administrative Code;
- (6) Complying with any state or federal program requirements;
- (7) Processing or payment of claims;
- (8) Auditing purposes;
- (9) Licensure processes, including determination of eligibility and filing requirements;
- (10) Investigation or law enforcement purposes;
- (11) Administrative hearings;
- (12) Litigation, complying with an order of the court, or subpoena;
- (13) Human resource matters, including but not limited to, hiring, promotion, demotion, discharge, salary or compensation issues, leave requests or issues, and time card approvals or issues;
- (14) Complying with an executive order;
- (15) Complying with an official commission policy or a state administrative policy issued by the department of administrative services, the office of budget and management or other similar state agency; or
- (16) Complying with a collective bargaining agreement provision.

(C) In addition to the general processes described in paragraph (A) above, in the following specific processes of the commission, authorized commission employees would have valid reasons for accessing confidential personal information:

- (1) Investigators, attorneys, and staff may review confidential personal information of individuals who are subject to investigation for alleged misconduct which may result in discipline. These same employees may review confidential personal information of individuals who are not the subject of the investigation, but may be witnesses with information related to the investigation. Confidential personal information may also be reviewed by these employees and members of the commission in professional conduct matters which become the subject of administrative hearings.

5.0 Confidential information.

(A) The following personal information maintained by the commission shall be confidential:

- (1) Social security numbers unless the individual was told that the number would be disclosed.
- (2) "Bureau of Criminal Identification and Investigation" criminal records check results in accordance with section 4776.04 of the Revised Code.
- (3) Investigative proceedings of the commission under section of the Revised Code.
- (4) Information that is considered confidential under section 149.43 of the Revised Code.

(B) All other personal information is considered a public record under section 149.43 of the Revised Code.

6.0 Restricting and logging access to confidential personal information in computerized personal information systems.

(A) Access to confidential personal information that is kept electronically shall require a password or other authentication measure.

(B) When the commission acquires a new computer system that stores, manages or contains confidential personal information, the commission shall include a mechanism for recording specific access by employees of the commission to confidential personal information in the system.

(C) When the commission modifies an existing computer system that stores, manages or contains confidential personal information, the commission shall make a determination whether the modification constitutes an upgrade. Any upgrades to a computer system shall include a mechanism for recording specific access by employees of the commission to confidential personal information in the system.

(D) The commission shall require employees of the commission who access confidential personal information within computer systems to maintain a log that records that access. Access to confidential information is not required to be entered into the log under the following circumstances:

- (1) The employee of the commission is accessing confidential personal information for official commission purposes, including research, and the access is not specifically directed toward a specifically named individual or a group of specifically named individuals.
- (2) The employee of the commission is accessing confidential personal information for routine office procedures and the access is not specifically directed toward a specifically named individual or a group of specifically named individuals.
- (3) The employee of the commission comes into incidental contact with confidential personal information and the access of the information is not specifically directed toward a specifically named individual or a group of specifically named individuals.
- (4) The employee of the commission accesses confidential personal information about an individual based upon a request made under either of the following circumstances:

(a) The individual requests confidential personal information about himself/herself.

(b) The individual makes a request that the commission takes some action on that individual's behalf and accessing the confidential personal information is required in order to consider or process that request.

(5) For purposes of this paragraph, the commission may choose the form or forms of logging, whether in electronic or paper formats.

(E) The commission shall issue a log management policy that specifies the following:

(1) Who shall maintain the log;

(2) What information shall be captured in the log;

(3) How the log is to be stored; and

(4) How long information kept in the log is to be retained.

3773-9-02 Personal information systems.

- (A) The executive director of the commission shall be directly responsible for the personal information system maintained by the commission.
- (B) The commission shall discipline any employee who initiates or otherwise contributes to any disciplinary or other punitive action taken against another individual who brings to the attention of appropriate authorities, the press, or a member of the public, any evidence of unauthorized use of any material contained in the personal information system.
- (C) The commission shall maintain its personal information system with the accuracy, relevance, timeliness, and completeness necessary to assure fairness in any determination made by the commission that is based on information contained in the system.
- (D) The commission shall investigate, upon request, the accuracy, relevance, timeliness, and completeness of the personal information which is disputed by the subject of a record contained in its personal information system and report its findings to the disputant within thirty days after receipt of the request.
- (E) The commission shall not place personal information into an interconnected or combined system unless said system contributes to the efficiency of other agencies or organizations authorized by law to use the system.
- (F) The commission shall not use any personal information placed into an interconnected or combined system by another state or local commission or an organization unless the personal information is necessary and relevant to the performance of a lawful function of the commission.

Procedures for accessing personal information.

- (A) Personal information systems of the commission are managed on a “need-to-know” basis whereby the information owner determines the level of access required for an employee of the commission to fulfill his or her job duties. The determination of access to confidential personal information shall be approved by the employee’s supervisor and the information owner prior to providing the employee with access to confidential personal information within a personal information system. The commission shall establish procedures for determining a revision to an employee’s access to confidential personal information upon a change to that employee’s job duties including, but not limited to, transfer or termination. Whenever an employee’s job duties no longer require access to confidential personal information in a personal information system, the employee’s access to confidential personal information shall be removed.
- (B) Upon the signed written request of any individual for a list of confidential personal information about the individual maintained by the commission, the commission shall do all of the following:
 - (1) Verify the identity of the individual by a method that provides safeguards commensurate with the risk associated with the confidential personal information;
 - (2) Provide to the individual the list of confidential personal information that does not relate to an investigation about the individual or is otherwise not excluded from the scope of Chapter 1347. of the Revised Code; and
 - (3) If all information relates to an investigation about that individual, inform the individual that the commission has no confidential personal information about the individual that is responsive to the individual’s request.
- (C) Upon discovery or notification that confidential personal information of a person has been accessed by an employee for an invalid reason, the commission shall notify the person whose information was invalidly accessed as soon as practical and to the extent known at the time. However, the commission shall delay notification for a period of time necessary to ensure that the notification would neither delay or impede an investigation of the circumstances and involvement of an employee surrounding the invalid access, nor jeopardize homeland or national security. Additionally, the commission may delay the notification consistent with any measures necessary to determine the scope of the invalid access, including which individuals’ confidential personal information invalidly was accessed, and to restore the reasonable integrity of the system. Once the commission determines that notification would not delay or impede an investigation, the commission shall disclose the access to confidential personal information made for an invalid reason to the person. Notification provided by the commission shall inform the person of the

type of confidential personal information accessed and the date(s) of the invalid access, and may be made by any method reasonably designed to accurately inform the person of the invalid access, including written, electronic, or telephone notice.

- (D) The executive director shall designate an employee of the commission to serve as the data privacy point of contact. The data privacy point of contact shall work with the chief privacy officer within the office of information technology to assist the commission with both the implementation of privacy protections for the confidential personal information that the commission maintains and compliance with section 1347.15 of the Revised Code and the rules adopted pursuant to the authority provided by that chapter.
- (E) The executive director shall designate an employee of the commission to serve as the data privacy point of contact who shall timely complete the privacy impact assessment form developed by the office of information technology.

3773-9-04 Valid reasons for accessing confidential personal information.

- (A) Pursuant to the requirements of division (B)(2) of section 1347.15 of the Revised Code, this rule contains a list of valid reasons, directly related to the commission's exercise of its powers or duties, for which only employees of the commission may access confidential personal information regardless of whether the personal information system is a manual system or computer system.
- (B) Any of the following functions normally performed by the commission constitute valid reasons for authorized employees of the commission to access confidential personal information:
- (1) Responding to a public records request;
 - (2) Responding to a request from an individual for the list of confidential personal information the commission maintains on that individual;
 - (3) Administering a provision of the United States constitution or Ohio constitution directly applicable to the operations of the commission;
 - (4) Administering a provision of Chapter 3773. of the Revised Code;
 - (5) Administering a provision of agency 3773 of the Administrative Code;
 - (6) Complying with any state or federal program requirements;
 - (7) Processing or payment of claims;
 - (8) Auditing purposes;
 - (9) Licensure processes, including determination of eligibility and filing requirements;
 - (10) Investigation or law enforcement purposes;
 - (11) Administrative hearings;
 - (12) Litigation, complying with an order of the court, or subpoena;
 - (13) Human resource matters, including but not limited to, hiring, promotion, demotion, discharge, salary or compensation issues, leave requests or issues, and time card approvals or issues;
 - (14) Complying with an executive order;
 - (15) Complying with an official commission policy or a state administrative policy issued by the department of administrative services, the office of budget and management or other similar state agency; or
 - (16) Complying with a collective bargaining agreement provision.
- (C) In addition to the general processes described in paragraph (A) of this rule, in the following specific processes of the commission, authorized commission employees would have valid reasons for accessing confidential personal information:
- (1) Investigators, attorneys, and staff may review confidential personal information of individuals who are subject to investigation for alleged misconduct which may result in discipline.
 - (2) These same employees may review confidential personal information of individuals who are not the subject of the investigation, but may be witnesses with information related to the investigation.

- (3) Confidential personal information may also be reviewed by these employees and members of the commission in professional conduct matters which become the subject of administrative hearings.

- (A) The following personal information maintained by the commission shall be confidential:
- (1) Social security numbers unless the individual was told that the number would be disclosed.
 - (2) Bureau of Criminal Identification and Investigation criminal records check results in accordance with section 4776.04 of the Revised Code.
 - (3) Investigative proceedings of the commission under section of the Revised Code.
 - (4) Information that is considered confidential under section 149.43 of the Revised Code.
- (B) All other personal information is considered a public record under section 149.43 of the Revised Code.

Restricting and logging access to confidential personal information in computerized personal information systems. .

- (A) Access to confidential personal information that is kept electronically shall require a password or other authentication measure.
- (B) When the commission acquires a new computer system that stores, manages or contains confidential personal information, the commission shall include a mechanism for recording specific access by employees of the commission to confidential personal information in the system.
- (C) When the commission modifies an existing computer system that stores, manages or contains confidential personal information, the commission shall make a determination whether the modification constitutes an upgrade. Any upgrades to a computer system shall include a mechanism for recording specific access by employees of the commission to confidential personal information in the system.
- (D) The commission shall require employees of the commission who access confidential personal information within computer systems to maintain a log that records that access. Access to confidential information is not required to be entered into the log under the following circumstances:
 - (1) The employee of the commission is accessing confidential personal information for official commission purposes, including research, and the access is not specifically directed toward a specifically named individual or a group of specifically named individuals.
 - (2) The employee of the commission is accessing confidential personal information for routine office procedures and the access is not specifically directed toward a specifically named individual or a group of specifically named individuals.
 - (3) The employee of the commission comes into incidental contact with confidential personal information and the access of the information is not specifically directed toward a specifically named individual or a group of specifically named individuals.
 - (4) The employee of the commission accesses confidential personal information about an individual based upon a request made under either of the following circumstances:
 - (a) The individual requests confidential personal information about themselves.
 - (b) The individual makes a request that the commission takes some action on that individual's behalf and accessing the confidential personal information is required in order to consider or process that request.

- (5) For purposes of this paragraph, the commission may choose the form or forms of logging, whether in electronic or paper formats.

(E) The commission shall issue a log management policy that specifies the following:

- (1) Who shall maintain the log;
- (2) What information shall be captured in the log;
- (3) How the log is to be stored; and
- (4) How long information kept in the log is to be retained.