Protection of Privacy Policy

Policy Number:	CLK-4
Approval Date:	January 13, 2026
Last Revised:	N/A
Policy Area:	Corporate Services – Clerk's Division
Policy Administrator:	Clerk
Keywords:	A17, information access, privacy, privacy breach

1 PURPOSE

1.1 The purpose of this Policy is to:

(a) outline The Corporation of Loyalist Township's ("Township") commitment to being open, accessible and transparent in its actions while protecting confidential information under its Control or Custody;

(b) outline operational directives in compliance with the Municipal Freedom of Information and Protection of Privacy Act ("M.F.I.P.P.A")., Personal Health Information Protection Act ("P.H.I.P.A"), and the Child, Youth, and Family Services Act and other applicable access and privacy legislation;

(c) ensure that video surveillance technology is used only for the administration of the Township's lawful duties and activities and provide clarity on when and how the Township may install and collect video surveillance footage; and

(d) establish reasonable measures which are defined, documented and put in place to prevent unauthorized access to the records of the Township as required by section 3(1) of R.R.O. 1990, Reg. 823.

2 SCOPE

2.1 This Policy applies to:

(a) all Township staff, including, but not limited to, full-time, part-time, casual, contract, volunteer and student/co-op placement employees;

(b) all vendors acting on behalf of the Township;

(c) all Personal Information which is collected, used, retained and disclosed by the Township.

(d) all Personal Health Information as defined by section 4 of P.H.I.P.A which the Township may, from time to time, receive from health information custodians as permitted by P.H.I.P.A.

Once PRINTED, this is an UNCONTROLLED DOCUMENT. Refer to the Corporate Drive for latest version

2.1 This Policy does not apply to:

(a) the interactions of Constituents with their elected Councillor, including the Mayor of the Township;

(b) information that is maintained for the purpose of creating a record that is available to the general public in accordance with legislation, by-law or policy;

(c) information associated with an individual in a professional, business or official capacity is not personal information. Business and professional information includes position title, business telephone number, business address, business email address, and opinions and recommendations expressed in a professional capacity; and

(d) Integrity Commissioner, Meetings Investigator and Auditor General, or to any employee acting under their instruction.

3 POLICY STATEMENT

Collection of Personal Information

3.1 Personal Information may only be collected in accordance with section 28 and 29 of M.F.I.P.P.A.,

(a) where the collection is authorized by statute or necessary for the administration of lawfully authorized activities such as delivery of services; or

(b) where a notice of collection in accordance with section 29(2) has been provided at the time the information is collected except as outlined in section 29(3) of M.F.I.P.P.A.

3.2 Identifying information about persons under the age of 18 is subject to the Child, Youth and Family Services Act, this Policy, and the Youth and Children Consent Procedures to ensure compliance with applicable legislation.

3.3 Pursuant to section 34(4) of P.H.I.P.A, the Township will not require individuals to produce their health card or accept the use of health cards to verify the identity of individuals in the proper administration of Township business.

3.4 The Township shall provide the notice of collection, as provided in Appendix A prior to the collection of any Personal Information.

Use of Personal Information

3.2 Personal Information shall be used for the purposes for which it was obtained in accordance to sections 31, 32, and 33 of M.F.I.P.P.A as illustrated in Appendix C.

Once PRINTED, this is an UNCONTROLLED DOCUMENT. Refer to the Corporate Drive for latest version

Disclosure of Personal Information

3.3 Personal Information under the Control or Custody of the Township will not be disclosed except in accordance with section 32 and 33 of M.F.I.P.P.A as outlined in the Access to Records Policy and as illustrated in Appendix C.

3.4 Personal or identifying information will not be disclosed to Artificial Intelligence third-party service providers.

3.5 Notwithstanding the above, pursuant to section 5 of the M.F.I.P.P.A, the Clerk has an obligation to disclose any record if the Clerk has reasonable and probably grounds to believe that it is in the public interest to do so and the record reveals a grave environmental, health or safety hazard to the public.

Personal Information Bank

3.6 Service areas are required to review and submit an index of Personal Information Banks, in the manner prescribed by the Clerk pursuant to section 34 and 35 of M.F.I.P.P.A and as outlined by Appendix B. The Personal Information Bank must be reviewed and updated whenever the collection, use or disclosure of Personal Information is introduced or changed.

Right to Access

3.7 Every individual has a right to access Personal Information about themselves contained in a Personal Information Bank, or under the Custody and Control of the Township pursuant to sections 37, and 38 of M.F.I.P.P.A.

3.8 Where the person making a request to access Personal Information is the individual named in the record and/or to whom the information relates, the request may be resolved subject to the Routine Disclosure described in the Access to Records Policy.

3.9 If the record contains Personal Information and the person seeking the Record is other than the individual named in the record, a formal F.O.I. request must be submitted unless the person making the request is authorized to access the information, or is the substitute decision maker under the Child, Youth, and Family Services Act.

Right to Correct

3.10 Pursuant to section 36(2) of M.F.I.P.P.A. and illustrated by Appendix D, an individual has the right to challenge the accuracy and completeness of their own Personal Information if the individual believes there is an error or an omission.

3.11 If it is demonstrated that any Personal Information is outdated, incomplete or inaccurate, it must be updated, completed and/or corrected at no additional cost. Staff may strikeout or clearly label the information that is deemed to be outdated, incomplete or inaccurate and take any corrective actions necessary.

Once PRINTED, this is an UNCONTROLLED DOCUMENT. Refer to the Corporate Drive for latest version

3.12 If there is a dispute about the currency, completeness or accuracy of the information in the record, the Clerk must be consulted, and the requester must be notified of their right to submit a request to correct Personal Information under section 36 of M.F.I.P.P.A.

3.13 The correction of personal information in a file does not necessarily entail the deletion or erasure of the original record. Rather, it may result in adding a note to a record or in the event of a continued dispute, the individual may attach an explanatory note or statement of disagreement to the information reflecting any correction that was requested but not made.

3.14 If the outdated, incomplete or inaccurate information has been shared with a third party within one year of the time that the correction was requested, then the third party may be notified at the request of the requestor of the updated, complete and/or accurate information or notified of the existence of the statement of disagreement.

3.15 If this is not satisfactory, the requester should be advised of his/her right to appeal pursuant to Part III of M.F.I.P.P.A.

Privacy Breach

3.16 A privacy breach occurs when Personal Information is collected, retained, used or disclosed in ways that are not in accordance with M.F.I.P.P.A.

3.17 When any apparent or suspected privacy breach occurs, staff must notify their Department Director, IT Manager and Clerk immediately upon becoming aware of the breach. Staff must take every necessary step to contain the breach immediately.

3.18 The Clerk shall investigate all reported, suspected or apparent breaches and provide support in the response, containment and remediation of breaches subject to the Privacy Breach Procedures.

Privacy Impact Assessment

3.19 A Privacy Impact Assessment in consultation with IT and the Clerk must be completed for the review or creation of any program or service that will result in the collection of Personal Information, and all recommendations must be implemented.

3.20 Each service area, in consultation with the Clerk and IT Division is responsible for establishing measures that include administrative, technical, and physical safeguards that are appropriate for the information's sensitivity, the format in which it is held, and the related privacy risks.

De-identification of Personal Information

3.21 De-identification is a practice that enables the Township to share information and report on statistics while minimizing risks associated with prolonged retention of, or exposure of identifiable personal information. Subject to the guidance of the Information Privacy

Once PRINTED, this is an UNCONTROLLED DOCUMENT. Refer to the Corporate Drive for latest version

Commissioner of Ontario, “once de-identified, a data set is considered to no longer contain personal information.” De-identification is governed by the following principles:

(a) privacy by design and by default embedded at the earliest stages of project planning;

(b) data minimization and proportionality such that the minimum necessary information is disclosed where possible; and

(c) accountability to periodically assess risk of re-identification of datasets.

3.22 Township staff must de-identify Personal Information in the following circumstances:

(a) statistical reporting and dashboards released internally or publicly;

(b) research or program evaluation involving Township data;

(c) open data releases on Township portals; and

(d) using third-party service providers i.e. analytics tools or Artificial Intelligence to analyze trends and datasets.

3.23 Township staff must consult with the Clerk if the dataset includes a small number of individuals, unusual or rare attributes or conditions, a high level of detail or if auxiliary datasets that can be linked in a manner that even after de-identification, makes it possible to infer or identify individuals whose data is being used.

Video Surveillance

3.24 Subject to section 28(2) of M.F.I.P.P.A, the Township shall exercise its authority to collect Personal Information through Video Surveillance to promote public and employee safety and to maintain the security of the Township’s assets and property. The Township shall do so:

(a) to enhance the safety and security of employees, the public and corporate assets;

(b) to detect, deter and investigate unauthorized or unlawful activities upon or involving Township property;

(c) to investigate and resolve claims of personal injury, damage, or serious misconduct to and other legal claims;

(d) for any other purpose consistent with the purpose for which the information was obtained; and

(e) by taking all reasonable steps to ensure that records are handled in a manner that provides continued security of the recorded information.

Once PRINTED, this is an UNCONTROLLED DOCUMENT. Refer to the Corporate Drive for latest version

3.25 The Township shall provide notice of the presence of installed video surveillance equipment by prominently posting signs at the perimeter of surveillance areas to ensure that reasonable and adequate warning that surveillance is or may be in-operation before entering an area that is within the video surveillance viewing area.

3.26 In recognition of the Township's commitment to transparency, the Township will make digitally available a copy of the notice of collection, and a list of all locations where video surveillance is installed through the Personal Information Bank.

3.27 The IT Manager shall establish a Video Surveillance Procedure that outlines the procedure to add CCTV cameras on Township properties, as well as restrict internal access to the Video Surveillance footage to Authorized Personnel.

3.28 Access to video surveillance footage by all other individuals is subject to the Access to Records Policy, and M.F.I.P.P.A.

Fees

3.29 The Clerk may assess fees for requests made under M.F.I.P.P.A pursuant to section 45 of M.F.I.P.P.A and as outlined in the Fees and Charges By-law.

4 RESPONSIBILITIES

4.1 Council is responsible for approving and making changes to the Policy.

4.2 The Department Directors are responsible for:

(a) ensuring all service areas within their departments maintain compliance with respect to privacy as set out in the Act, and ensuring all Personal Information is managed and protected;

(b) administering and communicating this Policy broadly to all employees in their service areas; and

(c) communicating to the Clerk and IT manager, pursuant to section 3.18 if there has been a breach of privacy.

4.3 The Clerk is responsible for:

(a) administering this Policy and creating procedures;

(b) maintaining and updating the Personal Information Bank Index as needed;

(c) monitoring compliance with the Policy;

Once PRINTED, this is an UNCONTROLLED DOCUMENT. Refer to the Corporate Drive for latest version

(d) providing guidance as to the process to submit a formal FOI request; and

(e) working with service areas in the event of a breach of privacy.

4.4 The IT Manager is responsible for:

(a) providing guidance on safeguards that protect the security of Personal Information in the Custody and/or Control of the Township;

(b) advising service areas during the Privacy Impact Assessment for the review or implementation of programs that collect Personal Information; and

(c) establishing and enforcing the *Video Surveillance Procedure* and monitor the Township for compliance with all provisions related to video surveillance.

4.5 Employees are responsible for:

(a) reviewing and complying with this Policy and M.F.I.P.P.A. in performing their duties and functions;

(b) assisting in responding to requests made under this Policy;

(c) consulting with their supervisor or the Clerk when there are uncertainties about disclosure and/or dissemination; and

(d) reporting to their supervisor pursuant to section 3.18 any unauthorized disclosure.

Compliance, monitoring and review

4.6 Review of the Personal Information Bank Index should be undertaken on an annual basis.

4.7 The Clerk is authorized to amend all appendices attached to this Policy as outlined in Section 8.

Reporting

4.8 Pursuant to section 26 of the M.F.I.P.P.A, the Clerk may report statistical information regarding the use of M.F.I.P.P.A., including but not limited to, the exercise of the Right to Access, Control or Privacy Breaches to the Information and Privacy Commissioner of Ontario on an annual basis by March 31. Service areas must ensure that the Clerk is aware of any request(s) which might impact the annual reporting requirements.

4.9 In the event of a privacy breach, the Clerk will determine the appropriate professional or regulatory bodies that should be informed of the breach. The Clerk must notify the Information Privacy Commissioner of Ontario if the privacy breach affects:

Once PRINTED, this is an UNCONTROLLED DOCUMENT. Refer to the Corporate Drive for latest version

(a) personal Information containing financial or health records of individuals;

(b) a large number of individuals (e.g. 50 or more);

(c) individuals under the age of 18, and/or information collected under the authority of the Child, Youth and Family Services Act;

(d) where the Privacy Breach has proven difficult for to contain without the assistance of the I.P.C.; or

(e) in the opinion of the Clerk in consultation with the Chief Administrative Officer it is determined that it is in the public interest to provide such a report.

Records management

4.10 All records relating to this Policy should be retained in accordance with the Information and Records Management By-law.

4.11 All records pertaining to Right to Correct must be stored in the same classification code, and subject to the same retention as the original Personal Information under dispute.

5 DEFINITIONS

5.1 Refer to Schedule “A” in the Information and Records Management By-law.

6 RELATED DOCUMENTS AND LEGISLATION

6.1 Access to Records Policy

6.2 *Child, Youth and Family Services Act*, 2017, S.O. 2017, c. 14, Sched. 1

6.3 De-identification Guidelines for Structured Data, Information Privacy Commissioner, October 2025

6.4 Fees and Charges By-law, as amended

6.5 Guidelines for the Use of Video Surveillance, Information Privacy Commissioner, October 2015

6.6 Information and Records Management By-law

6.7 *Municipal Freedom of Information and Protection of Privacy Act*, R.S.O. 1990, c. M.56, as amended.

6.8 Personal Information Bank Guideline

6.9 *Personal Health Information Protection Act*, 2004, S.O. 2004, c. 3, Sched. A

Once PRINTED, this is an UNCONTROLLED DOCUMENT. Refer to the Corporate Drive for latest version

6.10 Privacy Breach Procedure

6.11 Privacy Impact Assessment Guideline

6.12 Video Surveillance Procedure

6.13 Youth and Children Consent Procedures

7 FEEDBACK

7.1 Feedback about this document may be provided by emailing clerk@loyalist.ca.

7.2 To report suspected instances of noncompliance with this Policy, please see email clerk@loyalist.ca.

8 APPROVAL AND REVIEW DETAILS

Approval and Review	Details
Approval Authority	Council
Administrator	Clerk
Next Review Date	January 2031

Approval and Amendment History	Details
Original Approval Authority and Date	
Amendment Authority and Date	
Notes	

9 APPENDIX

Appendix A: Notice of Collection

Appendix B: Personal Information Bank Index (Template)

Appendix C: Use, Disclosure and Access of Personal Information

Appendix D: Right to Correct

Appendix E: Navigating Personal Information

This appendix is intended for members of the public and outlines the appropriate contact points with Township for navigating the disclosure, access and correction of their Personal Information.

Appendix F: Video Surveillance Signage Template

Once PRINTED, this is an UNCONTROLLED DOCUMENT. Refer to the Corporate Drive for latest version

Appendix A: Notice of Collection

Below is a sample of a Notice of Collection that can be adopted to the appropriate personal information bank, which pursuant to the Act, must be provided prior to the collection of Personal Information. Any deviations from the sample must be approved by the Clerk or designate.

Staff should review the **Youth and Children Consent Procedures** where the collection of Personal Information pertains primarily to persons under the age of 18.

Notice of Collection

Personal information is collected under the authority of [*cite section number and title of applicable legislation or by-law that authorizes collection/ activity/ or program*].

Personal information will be used by the [Division Name or "Township"] for the purposes of [*list principal purposes for which the information may be used i.e. administration of a program, for the purposes of contacting residents about a site plan application, etc. This must be the same as the purpose listed on the Personal Information Bank registry*].

[if the information is collected under the Child, Youth and Family Services Act, the notice must include the following:] Please note that you may give, withhold or withdraw consent to collect this information at any time.

Questions about this collection and use of your personal information may be directed to [*position title*] at [*telephone number*], [*mailing address*], [*email address optional*]."

Once PRINTED, this is an UNCONTROLLED DOCUMENT. Refer to the Corporate Drive for latest version

Appendix B: Personal Information Bank Index

On an annual basis, or upon the development or review of a program or service offering, each service area is responsible for the review of Personal Information Banks within the Custody and Control of the service area. Each service area is therefore responsible to provide the Clerk's Division with the following information:

(a) Name

(b) Location of Record (if Physical)

(c) Legal Authority to Collect the Information

(d) Personal Information Collected

(e) How the information is used on a regular basis

(f) To whom the information is disclosed on a regular basis

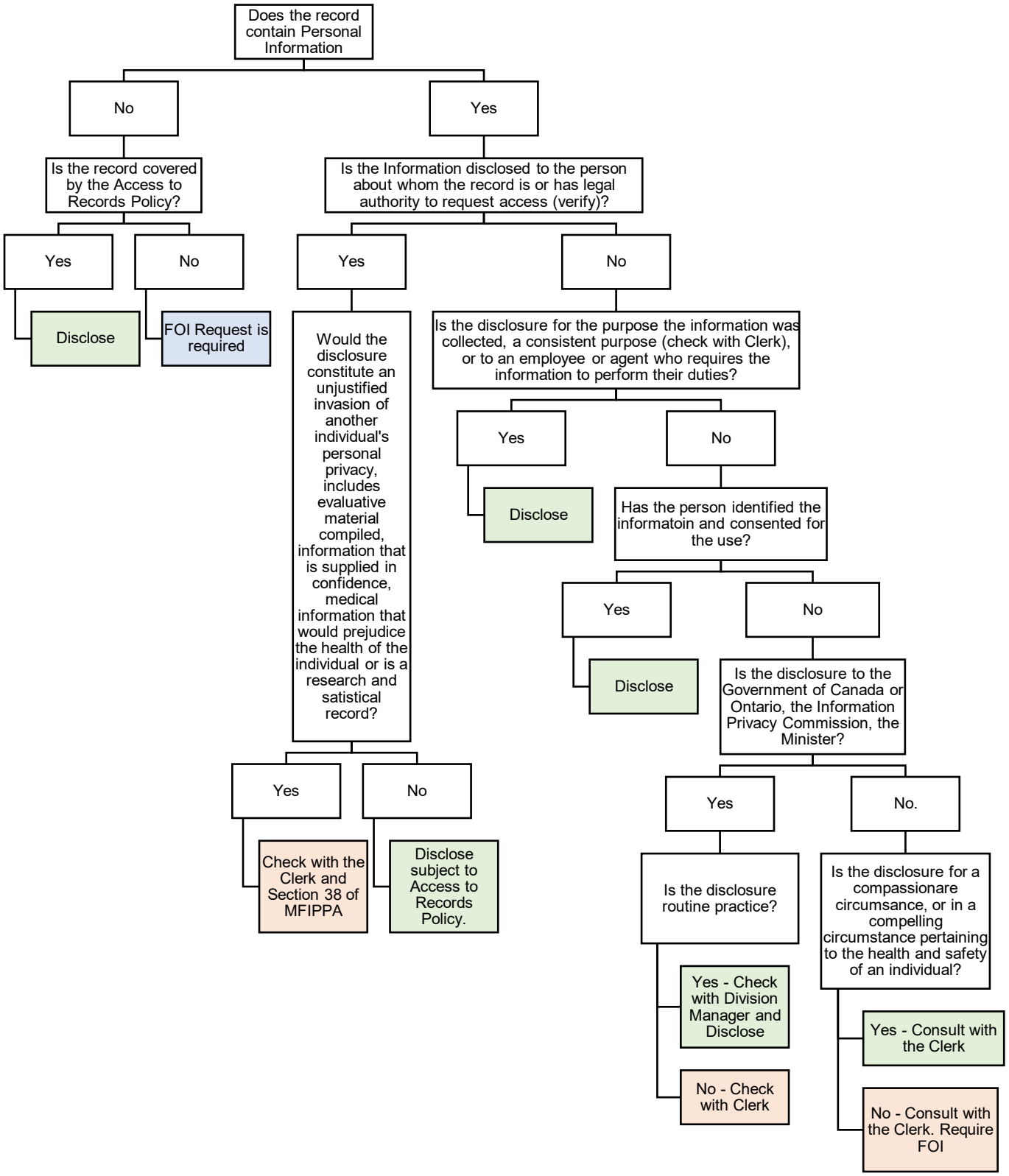
(g) Categories of individuals about whom personal information is maintained ex. the public, employees, council members, or individuals

(h) Classification Code, subject to the Township's Information and Records Management By-law

Staff should refer to the **Personal Information Bank Guideline** for further instructions.

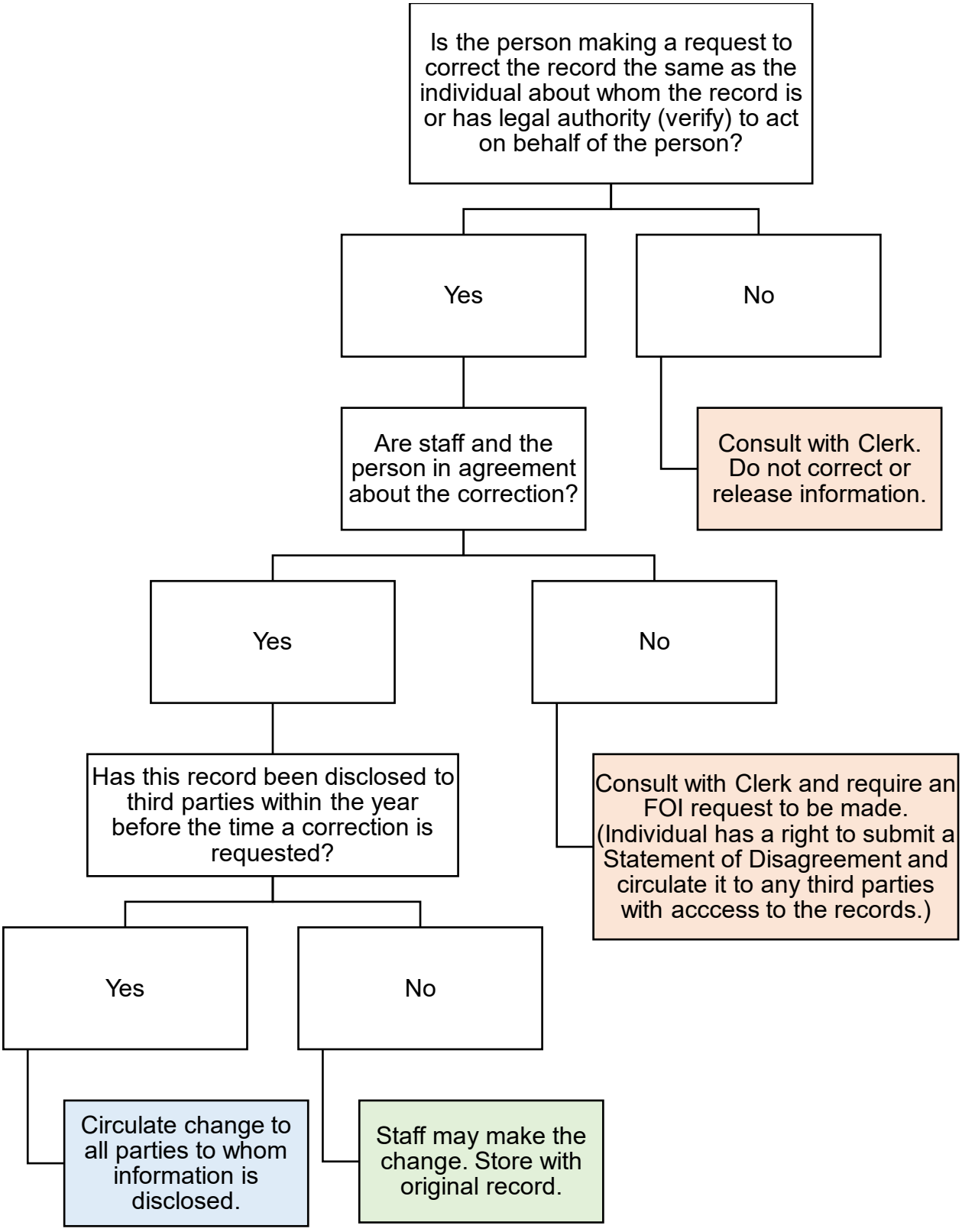
Once PRINTED, this is an UNCONTROLLED DOCUMENT. Refer to the Corporate Drive for latest version

Appendix C: Use, Disclosure and Access of Personal Information



Once PRINTED, this is an UNCONTROLLED DOCUMENT. Refer to the Corporate Drive for latest version

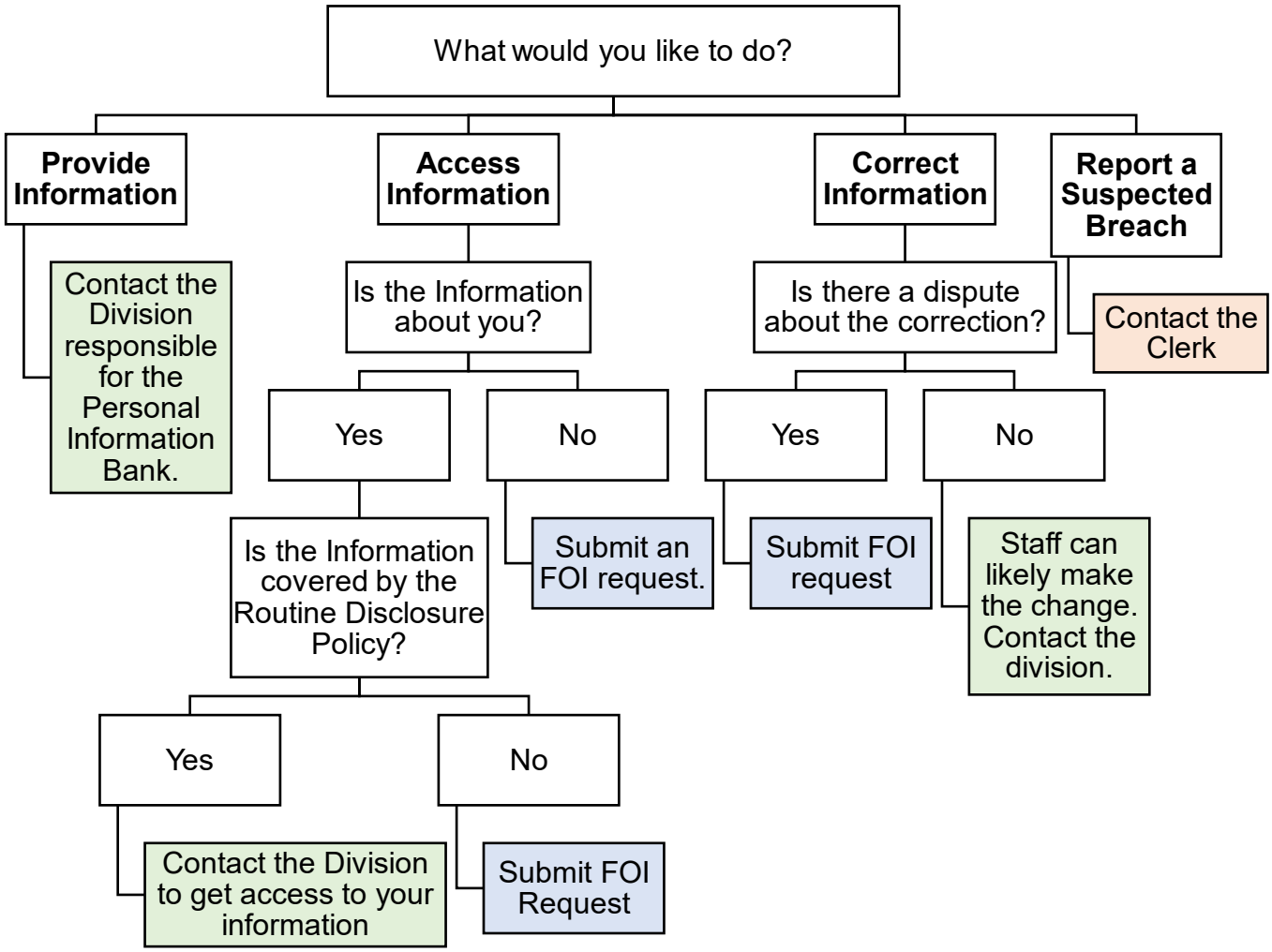
Appendix D: Right to Correct



Once PRINTED, this is an UNCONTROLLED DOCUMENT. Refer to the Corporate Drive for latest version

Appendix E: Navigating Personal Information

This appendix is intended for members of the public and outlines the appropriate contact points with Township for navigating the disclosure, access and correction of their Personal Information.



Once PRINTED, this is an UNCONTROLLED DOCUMENT. Refer to the Corporate Drive for latest version

Appendix F: Video Surveillance Signage Template



Once PRINTED, this is an UNCONTROLLED DOCUMENT. Refer to the Corporate Drive for latest version