

Public Records Request #2412

The following materials have been gathered in response to public records request #2412. These materials include:

- City of Charlotte Public Records Policy (ADM20)

This information was provided as a response to a public records request on 5/6/19 and is current to that date. There is a possibility of more current information and/or documents related to the stated subject matter.

Further Information

For further information about this request or the Citywide Records Program, please contact:

Cheyenne Flotree
Citywide Records Program Manager
City of Charlotte/City Clerk's Office
600 East 4th Street, 7th Floor
Charlotte, NC 28202
Cheyenne.Flotree@charlottenc.gov

Amelia Knight
Public Records Specialist
City of Charlotte/City Clerk's Office
600 East 4th Street, 7th Floor
Charlotte, NC 28202
Amelia.Knight@charlottenc.gov



Subject/Title
Public Records Policy

Date Effective
June 15, 2016

Revision Date Effective

Code Number
ADM 20



City Manager

City Manager's Office
Responsible Key Business

A. PURPOSE

The purpose of this Policy is to assist City of Charlotte (“City”) employees in understanding and complying with NC Public Records Law for record retention, disposition and record requests. This Policy will provide guidance and in the event of conflict between this Policy and the law, the law prevails. This Policy does not create any new or additional rights or obligations for any entity and does not create a higher standard than that created by existing public records laws. Personnel Records are an exception to the Public Records Act and the handling, retention, disposition, and response to record requests are handled as directed by City Human Resources and in accordance with State law, and are excluded from this policy.

This policy replaces 1.05 Municipal Records Access and Control, CLK2, Municipal Records Retention and Disposition Schedule, BSS9 Electronic Records Retention Policy, and ADM14 Charge for Copies of Public Records.

B. KEY DEFINITIONS

Board: All City non-elected, appointed bodies (includes all boards, commissions, committees, task forces, etc.).

Copyright: The legal right granted to a person for exclusive publication, production, sale or distribution of materials.

Employee: All City employees, including temporary, part-time employees. Volunteers, contractors, interns and persons working for a temporary employment service (“temps”) are also subject to this Policy, but the City employee supervising the volunteer or “temp” is also responsible for the public records of such volunteer or “temp.”

File Custodian: The employee responsible for managing a file or category of records (project or subject file) in accordance with the Records Retention and Disposition Schedule.

Departmental Records Management Liaison: The designated employee responsible for understanding and communicating expectations consistent with NC Public Records Law, coordinating, implementing and supervising departmental records management team and program, ensuring employee availability and participation in proper ongoing departmental training, and evaluating department performance ensuring adequate records management. The Departmental Records Management Liaison also monitors/manages public records requests in coordination with Communications Specialists, and ensures proper tracking in the Citywide Tracking System.

Network: A system by which computers are connected together. The City has a network that allows access to authorized areas on a central storage device and to access printers and shared drives.

Official(s): All City appointed board/commission, committee and task force members and paid employees.

Official Record Custodian (also referred to as “official custodian”): City Department Directors are responsible for all City business related records created/received by all staff in the Department (including the City Clerk for City Council business related records and Board Staff Advisors for Board member business related records).

Personnel Records: Information in any form (electronic, hard copy, email, voice messages, etc.) about a former or current City employee or applicant related to that employee’s performance or work for the City. This includes, but is not limited to, information regarding application, selection or nonselection, performance, promotions, demotions, transfers, suspensions, any other disciplinary actions, evaluation forms, leave, salary, and termination of employment.

Primary Record Custodian (also referred to as “record custodian”): Employees and officials who create and receive records are responsible for managing the records according to the Municipal and/or Department Records Retention and Disposition Schedule and disclosing the records upon request.

Protected Record: A record that is exempted from the definition of public records and a record for which there is statutory or other authority permitting or requiring that the information not be disclosed.

Public Record: All records, electronic or hard copy, created or received by City officials and employees while transacting official City business.

Record Request: Includes any request for records, including subpoenas and legal discovery.

Records Retention and Disposition Schedule (also referred to as “Schedule”): The City Council adopted Schedule that identifies and describes the City’s records and provides retention and disposition instructions as required by North Carolina Department of Cultural Resources.

Redact: To remove confidential or protected information from a record before releasing the record in response to a records request.

Retention: As used in this Policy, the minimum length of time the City will retain a record according to the Records Retention and Disposition Schedule.

Subpoena: An order of the court or an attorney requiring a witness to appear at a specified place and time to testify and/or to produce records. [Note: If a subpoena is for personnel records, Human Resources should be contacted.]

Transitory: Records that are ephemeral, temporary, or transient in nature and have only short-term administrative value.

C. PUBLIC RECORDS

1. Public Records Defined

With very few exceptions, all records created or received by officials and employees while transacting official City business are public records and must be retained, stored, disposed of, and made available for inspection and copying in accordance with the law. This applies to records in officials' and employees' homes and on home or personal computers if the record pertains to City business. The public records law is primarily contained in N.C.G.S.132-1 through N.C.G.S. 132-10, which is online at: http://www.ncga.state.nc.us/EnactedLegislation/Statutes/HTML/ByChapter/Chapter_132.html.

Public records include paper and electronic documents, photos, videos, maps, computer files, computer communications (i.e., email, instant messages, etc.), text messages, and voice mail messages. Unless the purpose and content of a record is personal in nature and not related to the transaction of City business, it is a public record and should be managed according to the Records Retention and Disposition Schedule.

There are several categories of public records including permanent, transitory, draft, and protected records. There are certain records that are exempted from the definition of public records, and there are certain public records that do not have to be disclosed.

2. Permanent Records

Permanent records should be maintained indefinitely in the office that created the records. Permanent records must also have a security preservation duplicate, which is either a paper or microfilm copy. Records scheduled for permanent preservation should not be destroyed without specific written permission from the NC Department of Natural and Cultural Resources.

3. Non-permanent Records

Non-permanent records may be retained in any format, and therefore you may be approved to destroy hard copy originals after being imaged in accordance with NC Department of Natural and Cultural Resources guidelines. You will have to take precautions with records that you must keep more than about 10 years. Computer systems do not have long life cycles. Each time you change computers systems, you will have to convert all records to the new system so that you can assure their preservation and provide access.

4. Transitory Records

Transitory records are public records that have limited value and do not have to be retained long-term. Transitory records include (but are not limited to) messages with short-term or no administrative value, such as many, but not all, voice mails, instant messages, text messages, self-sticking notes, facsimile cover sheets that do not contain substantive information, and telephone messages. Transitory records are created primarily for the informal communication of information and not to perpetuate or formalize knowledge. Transitory records do not set City policy, establish guidelines or procedures, discuss a City business matter, discuss a decision, certify a transaction, or act as evidence of receipt. (Certified or registered mail return receipts that contain important information about the names of the sender/recipient and pertinent dates are not transitory.) Transitory records may be treated as having a reference or administrative value that ends when the employee or official no longer needs the information in the record. Transitory records may be purged when their reference value ends. However, if a record request is received for a transitory record before that transitory record has been purged, that transitory record must be disclosed.

When a transitory record is related to personnel, an HR representative should be contacted to determine whether the information can be purged.

5. Draft Records

Draft records are preliminary records not yet in their final form. Once a draft document has been shared with another, it is a public record and is subject to public inspection. Inspection may be required for some uncirculated drafts. Officials and employees should consult with the City Attorney's office about the public record status of a draft document prior to denying inspection of that document.

To avoid misunderstandings that can sometimes arise from public circulation of discussion drafts, consider labeling each page of draft documents that you circulate to others with "DISCUSSION DRAFT ONLY." This can be done by going to the Microsoft Word Format menu, selecting "Page Layout", clicking on "Watermark", selecting "Custom Watermark" then "Text Watermark", typing in as the text: "Discussion Draft Only" and clicking on "apply" or by adding "Discussion Draft Only" to the footer of each page of draft documents.

6. Protected Records/Restricted Data

Protected records are records or data within records exempt from public disclosure rules. Protected records should not be disclosed, and in some cases must not be disclosed. Just as employees and officials have a duty to disclose public records, they have a duty to protect the privacy of protected records. In particular, a social security number must never be released as part of a public record. Make efforts not to include protected information and public information in the same record. Records that contain a mix of public records and protected records must be disclosed, but the protected information

Subject/Title

Public Records Policy

Code Number

ADM 20

Page

5

of

18

must first be removed (if on a separate page) or redacted (if on the same page with public information). (See Section F.2. of this Policy for more information on redaction.) When in doubt as to whether a record is a protected record, employees and officials should consult with the City Attorney's Office. Consulting with the attorney has advantages in the event you determine the record is protected and you do not disclose it, and there is a legal challenge (see Section F.5. of this Policy for more information on enforcement and penalties).

Exempted records (records that are exempted from public record disclosure) include but are not limited to:

- Confidential communications from the attorney to the client within the scope of the attorney-client relationship as defined in [N.C.G.S. 132-1.1](#) (which becomes public record in three years).
- Public enterprise billing information, as provided in [N.C.G.S. 132-1.1](#).
- Controlled substances reporting system information as provided in [N.C.G.S. 132-1.1](#) (which may be released only in accordance with The Controlled Substances Act).
- Criminal investigation records and records of criminal intelligence information, as provided in [N.C.G.S. 132-1.4](#) (note that certain information pertaining to violations of the law and arrests and indictments, and certain content of 911 calls are public records). Note also that certain information about violations or apparent violations of the law is a public record pursuant to [N.C.G.S. 132-1.4\(c\)](#).
- 911 database information, if required by agreement with the telephone company as provided in [N.C.G.S. 132-1.5](#).
- Sensitive public security information, including specific details of public security plans and arrangements, detailed plans and drawings of public buildings and infrastructure facilities, and certain plans to prevent and respond to terrorist activity, as provided in [N.C.G.S. 132-1.7](#), and technology security information.
- Certain identifying information of minors participating in a park or recreation program, although the zip code of residence is a public record, as provided in [N.C.G.S. 132-1.12](#)
- Other records for which statutory exemptions apply.

Records protected from disclosure include but are not limited to:

- Personnel files of employees, which includes any information gathered by the City with respect to an employee are protected, except for the following specific information that [NCGS 160A-168](#) requires to be public information: name; age; date of original employment or appointment; terms of any employment contract; current position title; current salary; date and amount of each increase or decrease in salary; date and type of each promotion, demotion, transfer, suspension, separation, or other change in position; date and general description of the reasons for each promotion; date and type of each dismissal, suspension or demotion for disciplinary reasons; copy of the written notice of final dismissal decision setting forth the specific acts or omissions that are the basis of the dismissal, and the office to which the employee is currently assigned.

Subject/Title

Public Records Policy

Code Number

ADM 20

Page

6

of

18

- Certain Law Enforcement and Emergency Management Staff information under [N.C.G.S. 160A-168](#) and [N.C.G.S. 132-1.7](#).
- “Tax information” pertaining to a taxpayer’s income or gross receipts may not be disclosed, as provided in [N.C.G.S.132-1.1](#), except as provided in [N.C.G.S. 160A-208.1](#) which permits disclosure to comply with a law or court order; for review by the Attorney General (“AG”) or representative of the AG; and to sort, process or deliver tax information for the City to administer a tax.
- Social security numbers and personal “identifying information” are confidential and unlawful to disclose to the public. Employees and officials must check with Human Resources before collecting any social security number. If a social security number is lawfully collected, on a City-generated form, it must be segregated on a separate page, or as otherwise appropriate, from the rest of the record, as provided in [N.C.G.S. 132-1.10](#). In addition to social security numbers, “personal identifying information” includes: employer taxpayer identification numbers; drivers’ license numbers (except in cases where the number appears on a non-protected law enforcement record), state identification card numbers and passport numbers; checking, savings, credit, and debit account numbers; personal identification code (PIN) numbers used to access financial resources; digital signatures; any other numbers or information that can be used to access a person’s financial resources; biometric data; fingerprints; and passwords; all as provided in [N.C.G.S. 132.1.10](#), [N.C.G.S. 75-61](#) and [N.C.G.S. 14-113.20](#).
- Trade secrets and electronic payment account numbers (see “identifying information” above for protection of account numbers) are protected as set forth in [N.C.G.S. 132-1.2](#). (Note that to protect a “trade secret” detailed requirements must be met.)
- The seal of an architect, engineer or land surveyor when that seal has been submitted for project approval under Part 5 of Article 19, Chapter 160A (Building Inspections) as set forth in [N.C.G.S. 132-1.2](#).
- Certain “trial preparation materials” are protected as provided in [N.C.G.S. 132-1.9](#). If records are created for or at the request of an attorney for the City when the City is engaged in litigation or litigation is anticipated, these records are likely protected “trial preparation materials.” The City Attorney’s Office should be consulted if there is a request for such records.
- Names and addresses of complaining witnesses to crimes must be temporarily withheld if release of the information is reasonably likely to pose certain threats to the witness or materially compromise the investigation, as provided in [N.C.G.S. 132-1.4](#).
- Certain economic development incentives are temporarily protected, but the City must make certain prior disclosures to applicants, as provided in [N.C.G.S. 132-1.11](#).
- Alarm System Registration Information under [N.C.G.S. 132-1.7A](#).
- Notwithstanding any other provision of law, all restrictions on access to public records expire 100 years from the date of the record’s creation under [N.C.G.S. 132-11](#), subject only to limitations therein.

See City Policy ADM13 Protection of Restricted Data for additional information and training on restricted data.

D. MUNICIPAL RECORDS RETENTION AND DISPOSITION SCHEDULE

The Municipal Records Retention and Disposition Schedule is issued by the Division of Archives and History, Department of Natural and Cultural Resources, and has been adopted by the City of Charlotte as its authority for the retention and disposition of records. The schedule groups records employees create or receive as a function of their job and provides retention and disposition instructions. (Departments may establish more detailed retention schedules that identify file custodians, methods and locations for the collection and storage of categories of records.)

- Records listed in this schedule, or added later by amendment, may be destroyed after the specified retention period without further approval by the Department of Cultural Resources or the governing body.
- Records may **not** be destroyed prior to the time periods stated, unless with the written permission of the NC State Archives.
- In the event that a legal requirement, statute, local ordinance, or federal program requires that a record be kept longer than specified in this schedule, the longer retention shall be applied.
- All provisions in the Schedule remain in effect until the schedule is officially amended.

E. RESPONSIBILITY FOR RECORDS

1. Current employees and officials

The law provides in [N.C.G.S. 160A-171](#) that the City Clerk is the custodian of all City records and in [N.C.G.S. 132-2](#) that the “public official in charge of an office having public records shall be the custodian thereof.” This Policy establishes the following record responsibilities:

- a. Officials and employees are the primary record custodians of all records they create, send and receive. Every primary record custodian is responsible for retaining, managing, and disclosing their records in accordance with the Schedule.
- b. Each Department Director is the official custodian of all records created, sent and received in his or her department, including those of former employees from that department.
- c. The City Clerk is the official custodian of all records created, sent and received by the Mayor and City Council members. City Council members may provide the Clerk all City business records. Once received, the City Clerk shall maintain, retain, and disclose such records upon a records request. The Mayor and City Council members remain responsible for, and shall maintain, retain, and disclose

all records not provided to the City Clerk in accordance with this Policy. The Mayor and Council members assigned staff shall assist in the management and maintenance of Mayor and Council members records, including correspondence, letters, and emails.

- d. The Staff Advisor of each board is the official custodian of all records created, sent and received by board members. Board and commission members may provide the Staff Advisor of their respective board all City business records. Once received, the appropriate Advisor shall maintain, retain, and disclose such records upon a records request.

Every official custodian is responsible for assuring that retention and disclosure requirements are met for the records of their department. Official custodians shall establish and maintain management, retention, and disclosure practices for their departments consistent with this Policy and the law. Official custodians shall receive records requests for records of their department and assure that the appropriate primary record custodians disclose the records.

Each primary record custodian is responsible for maintaining and managing the public records they create, send and receive in compliance with the Municipal Records Retention Schedule.

Retention responsibilities

The City employee or official who creates a record is responsible for managing the record according to the Schedule. Other employees and officials who receive copies of a record only need to keep it until its value to them ends. All City employees and officials are responsible for managing records they create and receive from outside the City of Charlotte, unless they designate the management of that record to a file custodian.

Generally, employees and officials who are copied on correspondence, unless they are the custodian of that main file, are not required to keep a copy of the record. If you are the only City employee or official copied on a correspondence, you are likely the custodian of that record and must manage it properly.

Use the chart below as a reference guide to determine who is responsible for keeping a particular record that is determined to be non-transitory. Refer to Section E.2., Litigation Hold Requirements, which outlines that employees and officials must keep all records when a lawsuit has been or is anticipated to be filed on a particular matter (even those records we would not typically keep).

| If the record is... | *Keep it | **Do not keep it |
|---|-----------------|-------------------------|
| Sent to you from an official/employee of the City | | X |
| Sent to you from someone outside the City of Charlotte (not | X | |

| | | |
|---|---|---|
| a City official or employee) | | |
| From you | X | |
| Sent from an official/employee of the City and you are cc'd | | X |
| Sent from someone outside the City of Charlotte (not a City official or employee) and you are cc'd | X | |
| Sent from an official/employee of the City and you are bcc'd | | X |
| Sent from someone outside the City of Charlotte (not a City official or employee) and you are bcc'd | X | |

* Or designate a file custodian

** After the record's administrative value to you ends

City employees and officials should not unnecessarily create or maintain multiple copies of any record, regardless of its medium. For example, if 10 photographs are taken for purposes of retaining one or two acceptable photos for business purposes, then the unsatisfactory photos are likely transient records and should be purged. Maintaining duplicates and transient records results in unnecessary expense to the City and creates a burden on the computer network. In the example given, if 10 unnecessary photographs are retained it has the undesired effect of possibly creating 10 new records.

The Innovation and Technology Department is responsible for computer system security and performance, but they are not responsible for managing employees' and officials' records. Each employee and official is the primary record custodian for their records, and each is responsible for managing City business related records according to the Schedule, regardless of whether they are stored on City-owned or personal equipment.

2. Departing Employee and Official Records

City business related records of departing employees and officials remain the property of the City. Failure of officials to deliver records to their successor or appropriate City employee upon demand is a Class 1 criminal misdemeanor, per [N.C.G.S. 132-4](#).

Departing Employee Records

The supervisor will:

- Advise the departing employee to manage all records (paper, electronic and telephone) according to the Schedule.

- Require the departing employee to review paper and electronic records to ensure file names are logical and meaningful and to ensure records are filed to provide for easy access and retrieval.
- Require that departing employee transfer any electronic records that are not stored on the City’s network to the appropriate location as designated on the Schedule prior to the employee’s last day of employment.
- Request the departing employee’s phone passcode to confirm that all voicemails have either been deleted or converted to a non-transient record form, as appropriate.

The employee will:

- Transfer any electronic records that are not stored on the City’s network to the appropriate location as designated in departmental File Plan.
- Purge duplicate hard copy records and clearly label any official reference documents in the office for easy access and disposition.

Innovation and Technology staff will:

- Move all departed employee’s email, home drive, and computer files to a permission-controlled location for review by the Department Director or designee for appropriate retention and disposition. These temporary copies will be available for disposition for 90 days.

Department Director will:

- Ensure all required duties are carried out. If the employee fails to carry out duties before departing, the Department Director or designee will review, manage, and transfer their records according to the Policy and the Schedule.

In the case of an employee termination or separation under unfavorable circumstances, the Department Director will ensure that the departed employee’s files are retained for a length determined by Human Resources in consultation with the City Attorney’s Office. (Typically, the length is 3 years.)

F. RETENTION AND DISPOSITION OF PUBLIC RECORDS

1. General Retention and Disposition Requirements

The law requires that public records be retained in a manner that allows public inspection and copying, and not destroyed for specific periods of time.

Any record that is retained electronically should be maintained in a secure system that controls access, storage, retrieval, alteration, and deletion. Each primary record custodian must set up their own retention and disposition procedures in compliance with department instructions to assure compliance with the law. File custodians should make records readily retrievable for staff so administrative copies are not necessary.

2. Litigation Hold Retention Requirements (See also City Policy ADM11, Litigation Records Preservation Policy)

A “litigation hold” is notice from the City Attorney’s office that a claim or lawsuit has been or is reasonably anticipated to be filed against the City. When a litigation hold notice is sent, ALL records that legal counsel deems to be relevant to the claim or lawsuit must be retained, and not purged, until the matter is resolved. Transient records (including telephone voice mail messages), duplicate records, electronic versions of printed records and other records for which there is no duty to retain under the Schedule must be retained once a litigation hold is issued.

The City Attorney’s office may need to issue a litigation hold if an official or employee receives a letter or other notice from an attorney for an adverse party that specific records be preserved. The City Attorney’s office should be consulted if such notice is received.

Employees shall retain records subject to litigation hold until otherwise notified by the City Attorney’s Office.

3. Records Disposition

Public records should be destroyed after they have been retained for the correct time period according to the Schedule by utilizing approved destruction methods outlined in the Schedule, unless there is some other reason that record should be retained, such as an outstanding record request or litigation hold.

A public record that is not properly purged remains a public record and must be disclosed upon request. For example, if the Schedule requires the custodian maintain a record for two years and the custodian elected to retain the record for an additional year, the record must be disclosed should a record request or court order be received seeking the record. Having a plan for the destruction of records eliminates obsolete records and saves resources by not indefinitely and unnecessarily storing records beyond appropriate retention periods.

G. RECORDS REQUESTS

1. Responding to a Record Request

The law requires every record custodian to permit the inspection of any public, non-protected record in the custodian's custody at reasonable times and under reasonable supervision, and to furnish copies as promptly as possible. (See Section F.4. of this Policy

Subject/Title

Public Records Policy

Code Number

ADM 20

Page

12

of

18

for more information on fees City employees and officials may charge to produce records in response to a record request.)

Persons requesting to inspect a record cannot be required to disclose their purpose or motive for seeking the record, nor can they be required to give their name or address, or show an ID, or sign for a record. However, according to [N.C.G.S. 132-10](#), employees and officials may require the requesting party to agree in writing that geographical information system databases and data files will not be resold or used for trade or commercial purposes. Also, the City may require computer database requests be in writing according to [N.C.G.S. 132-6.2](#).

All requests for existing City records by individuals or organizations are considered a Public Records Request. All such requests must be tracked in the Citywide Public Records Request Tracking system, with the exception of requests that are routine in nature and commonly fulfilled during the course of normal business. (See [reference guide](#) located in the Records Management Team Site.) Departmental Records Management Liaisons should be made aware of public records requests in order to coordinate, manage tracking, and support fulfillment.

Departmental Records Management Liaisons and other employees and officials should immediately advise the Corporate Communications Director of any record request from the media or that pertains to sensitive or controversial issues (see ADM5 Media Relations Policy and Protocol).

The City employee who is responsible for working with the requester should confirm that the requester has fully and clearly identified the record(s) sought. Asking for, but not requiring, the request to be in writing may facilitate obtaining clear requests.

The City employee who is responsible for fulfilling records requests should make or direct a thorough search for all relevant records and provide one of the following responses within the originally agreed upon response time: (1) inform the requester that more time is needed to respond to the request and provide an estimated timeframe for the response; (2) make the record available for inspection or copying (redacted, if necessary – see Section F.2. of this Policy for more information on redaction), taking necessary precautions to ensure the records are not at risk of being lost, damaged or destroyed; (3) if there is no record, provide a written statement that a search of the records has been made and that no relevant record(s) exist (the law does not require record custodians to create a new record to satisfy a request); or (4) if the City Attorney concurs with denying the record request, or portions thereof, provide a written explanation of the basis for the denial.

In some cases, the responsible City employee may be able to simply forward a copy of the requested record(s) to the requester. In other cases, the record may be made available for inspection by copying those records identified by the requester (see Section F.4. for more information on the fees City may charge).

At the City Manager's Office or City Attorney's Office discretion, the Chief Security Officer may be requested to conduct a search of electronic records located on the network. Scenarios when this path might be warranted include requests of records from numerous people, complex search requests, or requests that may need to be treated as sensitive.

Copies of public records should be provided to the requesting party in the medium of the requester's choice, provided that the City is capable of satisfying the request in that particular medium (i.e., paper, CD/DVD, etc.). The person responsible for handling a request should communicate any anticipated cost and obtain approval from the requesting party prior to producing any records in response to the record request. The requesting party shall pay any cost prior to employees and officials reproducing records or at the time of receiving the records. If the requesting party does not concur with paying the fees, then the employee or official should work with the requester to make other arrangements for the inspection of records.

Employees and officials must allow the inspection of email addresses on electronic subscriber lists. However, employees and officials of the City of Charlotte are not required to provide a copy of these lists in response to a records request.

2. Redacting Protected Information

If a record subject to a records request is a protected record, employees will likely not have to make that record available for inspection and copying. In some cases, however, a public record will contain information that is protected, but the entire record is not protected. In those cases, the protected information should be deleted in a manner that shows that a deletion was made. This is called redacting. For example, if the record is a printed record, make a copy of the record, tape over the protected information with white correction tape, then use a black painter pen to completely mark over the tape. The marked up record should then be copied and the new redacted copy made available for inspection and copying. The custodian should save the electronic document as a new file name, and from the new file, black out the redacted data, using whatever highlighting tools are available in the document editing software (Microsoft Word, Adobe Reader, etc.), then print the document, and scan it back in (printing and re-scanning removes the actual text data hidden behind the highlighting).

3. Copyrighted Records

There are records in the City's custody that may be copyrighted material and protected by copyright laws. If a record request is made for a record that is protected by copyright, employees and officials should consult with the City Attorney's office prior to making the record available to the requester for inspection.

It is possible that City records may contain copyrighted materials for which employees and officials are not aware of the copyright status. If it is possible that records provided by employees and officials may include copyrighted materials, then the employee or

official should use the following statement when releasing the records in response to a records request:

The City is providing copies of records you have requested in accordance with the North Carolina Public Records Law. To the extent any of the records provided are copyrighted, take notice that these records remain subject to copyright law and you are not authorized to reproduce, download or otherwise reproduce or copy any copyrighted material or work that the City has provided in accordance with the public records law. The use, reproduction, downloading or distribution of copyrighted materials and works may subject you to applicable penalties and damages under state and federal laws.

4. Charging for Producing Records

N.C.G.S. 132-1 permits the City to charge a fee for copying a record that recovers the actual cost of producing the record. In rare cases, providing public records may require extensive use of information technology resources or clerical and/or supervisory assistance. In these cases, the official custodian may assess a reasonable service charge based on the City's actual incurred costs pursuant to N.C.G.S. 132-6.2. This reasonable service charge must be approved by the Department Director and the City Manager or designee. An estimate of the charges should be given to the requester and approval obtained prior to responding to the request.

To the extent practical, all fees and charges should be collected before producing the records or at the time the records are delivered.

5. Disputed Records Requests: Enforcement and Penalties

The law provides a mediation process for resolving lawsuits regarding public records disputes. The law also provides that if a legal action is brought against the City to compel the disclosure of public records, the City will be required to pay the other party's attorney's fees if the other party substantially prevails in the action unless the court finds that the City acted in reasonable reliance on (i) certain court orders or judgments applicable to the City, (ii) a published appellate court opinion or (iii) a written opinion or letter of the NC Attorney General. Individual employees and officials are not subject to personal liability for attorney fees if they consulted with and followed the advice of an attorney. For this reason, if employees or officials have doubts about the protected status of a record or are considering denying a records request, they should consult the City Attorney's office.

H. GENERAL RECOMMENDATIONS

- Make thoughtful decisions about the medium you use to convey information. The creation and retention of unnecessary printed and electronic records places burdens

Subject/Title

Public Records Policy

Code Number

ADM 20

Page

15

of

18

- on the City's physical and electronic storage systems. Avoid creating records that are not necessary, and dispose of unnecessary duplicate records and transitory records.
- Try not to mix public records with protected and personal records. Treat protected records with a heightened concern for security, and segregate protected records from other records if possible. Never share protected records with a person who should not have access to those records. In some cases, such as with Social Security numbers, the law requires that the protected record be segregated.
 - Maintain all City records on City equipment and all personal records on personal equipment.
 - Time spent creating a record retention and disposition management system that meets the requirements of this Policy and works for the custodian is time well spent. Appropriately label and store records so they can quickly and easily be retrieved in the event a records request is received. Label those records that are protected records or that contain protected records in a manner that clearly indicates their protected status. If a protected record will become a non-protected record at some time in the future, mark it in some way to identify the date protected status will end. Dispose of transitory records, duplicate records, and records that have exceeded their retention period.
 - Contact the Public Records Administrator/Project Manager, City Clerk or City Attorney's office with any questions about this Policy.
 - Contact Corporate Communications and advise them of media record requests.

I. RELATED DOCUMENTS

- North Carolina General Statutes ([Chapter 132](#) and other chapters)
- [Records Retention and Disposition Schedule](#)

Appendix A: Using Technology for Records Management

The policy language above speaks to parameters for handling of all records, regardless of what form they take; paper or electronic. Below is some guidance and requirements for how best to use City of Charlotte technologies to accomplish these records management goals for electronic records. In the coming months, improvements may be made to our technologies to further facilitate our organizational records management goals.

Email

Staff Should Send Links Rather than Attachments in Email: Generally speaking, email should be used for communication, not for file storage. Wherever possible, if you have files you need to keep as a record, put them in a file storage location (G: drive, H: drive, SharePoint, etc.) and reference them in the email by sending a link rather than attaching the file directly. This also helps reduce duplication of data across the enterprise. You'll need to be aware of file permissions when using this approach. If someone doesn't have read access to a file that you've shared a link to, they will not be able to view it.

Staff Should Store Email in Folders Organized by Year or Retention Period: Emails are to be retained as records should be categorized into email folders in the same way an employee would file a paper version in their area (i.e. in folders by fiscal year, by project, contract, etc.). This gives users the chance to move emails to the proper network storage folder, or other electronic management system when correspondence becomes inactive. Correspondence can then be filed in the folder along with other related documents for a more complete record and labeled according to retention period (1 year, 5 years, 30 years, etc.). Sub-folders can be created under the retention folders to further categorize records by subject if more granularity is desired/required.

Staff Should Not Use .pst Files without Permission: Some staff may currently be using personal mailbox (.pst) files for storing email outside of the City's email server. As usage of these files makes discovery (and lost email recovery) more difficult, employees **should not** use these files without permission from your Department Director and the City's Chief Security Officer. Employees that are currently using them, should move email from those files back into the email server, using email folders as described above and remove the .pst files once emptied. It is anticipated that use of these files will be systematically disabled at some point in the near future.

Staff Shall Not Use Personal Email Accounts for City Business: Finally, employees are not permitted to use personal email accounts (a private, non-City account such as yahoo, gmail, etc.) to conduct City business unless City email is unavailable. City email can be accessed from any computing device with internet access unless the City's email system is down, so this should be rare. Any employee with a business need has access to City email and should use that account for all City business. In addition to making discovery nearly impossible, external email usage is also already limited in the City's Information Security Policy Manual to avoid unintentional distribution of sensitive information. If City email is unavailable, and an email

must be sent from a personal account, staff's City email account should be copied in the communication.

Personal Storage

Staff Shall Not Store City Records on Personal Storage: Employees are not permitted to use personal, non-City storage for storing City records. This includes non-City issued versions of the following; personal computers, external drives, thumb drives, and cloud storage services like Dropbox or Google Docs. If staff uses cloud storage for collaboration on working drafts with outside of City entities, records must be moved to one of the recommended locations for management and storage through the life of the record. This transfer of documents must occur, as Cloud based storage is disallowed in the City's Information Security Policy Manual for security reasons. Internal storage is available for everyone with a business need, and corporately-managed cloud storage (Microsoft OneDrive) is preferred and is available for a small annual subscription fee.

Staff Shall Not Store City Records on the Public Website: The City's extranet or public website is not an approved storage location for official City records. All official records published for access by the public, must be stored internally by the office of record.

Direct PC / Laptop / Tablet Storage

Staff Shall Not Store City Records Directly on City-Issued Computers: Data stored directly on the PC / laptop / tablet (the C: drive) is difficult to do records discovery against. It also is not recognized by any of our backup mechanisms, and therefore is not recoverable. For these reasons, storing records *only* on these devices is not permitted. It is fine to *copy* a document to one of these for temporary / offline work, as long as the record is returned to a discoverable location once that work is complete.

Network Storage – S: drive, H: drive, G: drive, etc.

Staff Should Use Network Storage by Default: Everyone's computer has a C: drive – that is the computer's local storage. In addition to this, most City users will also see other drive letters that represent enterprise storage made available for local use. For most people, G: or K: is a departmental shared drive, H: is a private "home" drive, and S: is a Citywide shared drive. Other drive letters may also be visible – their usage varies from department to department. These network drives should be the default storage location for files that aren't otherwise a better fit elsewhere (SharePoint, OneDrive, etc.). In particular, large files, personal files, or files that are relevant only to your department or division are probably a good fit for network drives.

SharePoint

Staff Should Move SharePoint Files Before Removing a Team Site: In addition to being an enterprise platform for internal marketing websites, departmental news, contact information, etc., SharePoint is also a collaboration tool and is especially useful in cross-departmental team

scenarios. Often these teams are temporary, like a project team. For these scenarios, the site owners should be mindful to transition files with retention periods that exceed the life of the team to a longer-term location, such as the file system.

Text Messages / Instant Messages

Staff Shall Forward Messages Deemed to be Records to their City Email: In many cases text messages and instant messages will be transitory, meaning they do not have to be retained. It is possible however, to create public records in either text message or instant message form. As with all records, it is the individual's responsibility to make that determination, and in those cases, that individual needs to forward the relevant text messages / instant messages to their City email account, so their retention can be managed in the same manner as and alongside their email records.