NORTH TAWTON TOWN COUNCIL

14a The Square
North Tawton
EX20 2EP

Tel: 01837 880121
e-mail: townclerk@northtawtontowncouncil.gov.uk

This is a document that sets out North Tawton Town Councils approved and agreed practices. Any deviation must be by resolution of the full Council.

DOCUMENT NAME:	Data Security and Breach Policy
Approved and Ratified date:	01/07/2025
Minutes Reference:	061:25/26
Review date:	July 2027
Version no:	V2

Version	Point(s)	Description of Change	Date

THIS IS A CONTROLLED DOCUMENT

Whilst this document may be printed, the electronic version maintained on the North Tawton Town Council website is the controlled copy. Any printed copies of this document are not controlled.

Contents

1 Purpose

1.1 Information is a major asset that North Tawton Town Council has a duty and responsibility to protect.

1.2 The purpose and objective of this Information Protection and Data Breach reporting policy is to specify the means of information handling and transfer within the Council.

2 Scope

2.1 The Information Protection Policy applies to all Councillors, Committees, Employees of the Council, contractual third parties and agents of the Council who have access to Information Systems or information used for North Tawton Town Council purposes.

2.2 Information takes many forms and includes:

- hard copy data printed or written on paper
- data stored electronically
- communications sent by post / courier or using electronic means
- stored tape or video
- speech, including social media, livestreaming and recording by any means.

3 Information Storage

3.1 Information will not be held that breaches the **Data Protection Regulations 2018** or formal notification and guidance issued by North Tawton Town Council.

3.2 Records management and information retention policies will be followed.

3.3 Databases holding personal information will have a defined security and system management policy for the records and documentation.

3.4 This documentation will include a clear statement as to the use, or planned use of the personal information.

4 Disclosure of Information - Computer and Paper Based

4.1 The disclosure of personal information to other than authorised personnel is forbidden. If there is suspicion of a Member or employee treating confidential Council information in a way that could be harmful to the Council or to the data subject, then it is be reported to the Data Control Officer (Town Clerk) who will take appropriate action. If the data breach originates from the Clerk, then the Chair will be informed.

4.2 Printed information from premises without the express consent of the information owner. Consent will only be given in exceptional circumstances.

4.3 Protectively marked, personal or sensitive documents are not to be left unattended and, when not in use, are to be locked away and accessed only by authorised persons.

4.4 Disposal methods for waste computer printed output and other media must be in accordance with North Tawton Town Council's document policy and will be shredded and / or destroyed.

4.5 Distribution of information should be via the most secure method available.

5 Disclosure of Information – Telephone and E-mail

5.1 Where this involves the exchange of sensitive information then the following procedures will be applied:

6 Telephone calls:

6.1 Verify the identification of persons before disclosing information. If in doubt, return their call using a known telephone number.

6.2 Ensure that you are authorised to disclose the information requested.

6.3 Ensure that the person is entitled to be given this information.

6.4 Ensure that the information you give is accurate and factual.

7 Disclosure of information by email:

7.1 Personal or sensitive information is at risk, the email will be delivered through the public network and the message may be left at several locations on its journey and could be deliberately intercepted.

7.3 Email should not be used for sending personal or sensitive information unless in accordance with North Tawton Town Council Policies

7.4 The sender should be satisfied of the identity of the recipient, if in doubt the email should not be sent, and alternative methods should be used. Councillors and employees are encouraged not to use the auto-infill of addresses in the address field of emails to avoid mistakes.

7.5 No identifiable personal information should be included when sending on emails unless permission is given in writing by the original sender. Emails should not be forwarded without the consent of the original sender.

7.6 All Councillors will be issued with a dedicated Cllr Email address which is to be used for all Council business. Use of personal email accounts for Council business is strictly forbidden. North Tawton Town Council emails will carry a disclaimer

8 Sharing of Personal Information

8.1 Information relating to individuals shall not be shared with other authorities without the agreement of the Data Control Officer (Town Clerk).

8.2 Councillors and Staff should be aware of their responsibilities to be able to justify the sharing of information and to be able to maintain security when transferring information in person, by email, phone or post.

9. Data breach procedure

9.1. Introduction
If personal data held by the Council is mishandled, the law requires that it respond in certain ways. This document sets out how the Council will meet its legal obligations should such a situation ever arise.

9.2. What is a data breach?
The mishandling of personal data ("a data breach") can happen in many ways. The following list describes some of the most common (it is not a complete list):

- Sending or copying an email to an unintended recipient.
- Copying an email to recipients using "cc" rather than "bcc";
- Accidental loss or theft of a memory stick, laptop computer, CD-ROM, etc.
- Unauthorised persons gaining access to physical or electronic records (e.g. during a burglary or computer hack).
- Accessing records for no proper purpose (e.g. staff and councillors may need to consult records for a legitimate purpose, but it may be illegal for them to do so out of idle curiosity).
- Improper deletion or alteration of records (including by malicious persons or software);
- Ignoring or mishandling a legitimate request for data to be corrected or deleted.

Sometimes it is obvious when a data breach has happened, but this is not always the case. In case of doubt (that is, if you think that a data breach may have happened but are not necessarily sure) then you must follow this procedure.

9.3. Who does this procedure apply to?

- If you work for the Council (whether as an employee, a worker, or a free-lancer or contractor) then this procedure applies to you. Failure to do so without a lawful excuse may result in disciplinary or enforcement action being taken against you. In a sufficiently serious case this could result in dismissal without notice or immediate termination of your contract for services.
- Councillors are also required to conduct themselves in accordance with this procedure. Failure to do so without a lawful excuse or impeding staff in the application of the procedure may amount to a breach of the Code of Conduct.

9.4. What to do if a data breach is known or suspected
If you have reason to believe that a data breach has happened or may have happened, you **MUST** complete a Data Breach Report Form (see form below) as this

form details the procedure and the appropriate response to the data breach. The form will then be kept confidentially at the Council Office for council records only.

Do not worry if you cannot fill in every part of the form fully – fill in as much as you can. It is important not to delay for any reason – this is more important and urgent than anything else you may have to do (apart from medical emergencies or immediate threats to someone's physical safety)

Send the completed form to the Town Clerk and Deputy Clerk as soon as you can by email. If this is not possible, deliver hard copies to them in person at the council office.

9.5. Responding to a Data Breach Report

- Upon receiving a Data Breach Report Form the Town Clerk and the Deputy Clerk will speak to each other and agree which of them will take responsibility for the subsequent handling of the matter. Where this is not possible responsibility will fall on the Town Clerk unless they are unavailable for any reason in which case responsibility shall devolve to the Deputy Clerk.
- The responsible officer will then invoke and follow the Data Breach Checklist & Action Plan set out below.
- The Town Clerk will invoke and follow the Data Breach Checklist & Action Plan set out below.

Adopted: 01.07.2025
Minute Reference: 061:25/26
Review Date: July 2027.

NORTH TAWTON TOWN COUNCIL – Data Breach Report form

Details of breach (Describe briefly what has happened or how the data breach arose with dates and times where possible)	
Nature and content of data involved (Describe the type(s) of personal information involved e.g., email addresses, payroll information, medical information, etc.)	
Number of individuals affected.	
Name of person making this report.	
How and to whom this report was submitted	
Date and time this report was submitted.	

NORTH TAWTON TOWN COUNCIL - Data Breach Checklist & Action Plan

Date and time of Notification of Breach	
Notification of Breach received from Name Contact Details	
Report form attached.	
How and when report acknowledged	
Name of person investigating breach Name Job Title Contact details Email Phone number Address	
Further information about breach (not contained in report form)	
Information Commissioner informed if relevant	

Time and method of contact https://report.ico.org.uk/security-breach/	
Police Informed if relevant Time and method of contact Name of person contacted Contact details	
Individuals contacted How many individuals contacted? Method of contact used to contact. Does the breach affect individuals in other EU member states? What are the potential consequences and adverse effects on those individuals? Confirm that details of the nature of the risk to the individuals affected: any measures they can take to safeguard against it; and the likely cost to them of taking those measures is relayed to the individuals involved.	
Staff briefed	

Assessment of ongoing risk	
Containment Actions: technical and organisational security measures have you applied (or were to be applied) to the affected personal data	

Recovery Plan	
Evaluation and Response	