



Clear Desk and Clear Screen Policy

Date of adoption	25 th November 2026 Minute Number 26/11()
Reviewed	
Next Review Date	As required
Reviewed By	Policy & Resources Committee 21 st October 2026

Clear Desk and Clear Screen Policy

1. Purpose

Newton Abbot Town Council is committed to protecting confidential, personal and sensitive information and maintaining a professional and secure working environment.

This policy establishes simple requirements for keeping desks, workspaces and computer screens secure, particularly when they are unattended and at the end of the working day.

The purpose of the policy is to reduce the risk of information being lost, viewed, removed or disclosed without authorisation, while maintaining a practical working environment for staff.

2. Scope

This policy applies to all employees, councillors, volunteers, contractors and other persons who use Council workspaces or IT equipment.

It applies to Council offices, meeting rooms, reception areas and other workspaces where Council information is handled.

3. Clear Desk Requirements

Staff are not expected to maintain completely empty desks throughout the working day. Documents and materials required for current work may remain on desks while they are actively being used.

However, confidential, personal or sensitive information must not be left unattended where it could be viewed or accessed by an unauthorised person.

When leaving a workspace for an extended period, and at the end of the working day:

- Confidential or sensitive documents must be stored securely in an appropriate drawer, cupboard or filing location.
- Documents containing personal information must not be left openly visible.
- Keys, access cards and other security items must be stored securely where appropriate.
- Passwords, PINs or other login information must never be written down and left openly accessible.
- Council stamps, payment information or other items that could be misused should be secured.
- Unwanted confidential documents must be securely shredded. They must not be placed in ordinary waste or recycling bins.
- General paperwork, stationery and working materials should be left reasonably tidy to maintain a professional and safe working environment.

4. Clear Screen Requirements

Computers and other Council devices must be secured whenever they are left unattended.

Staff must:

- Lock their computer when leaving their workstation, even for a short period.
- Log out or shut down equipment at the end of the working day where appropriate.
- Avoid leaving confidential or personal information displayed on screens where it can be viewed by visitors or members of the public.
- Close documents and systems containing sensitive information when they are no longer required.
- Ensure passwords are not shared or displayed near the workstation.

On Windows computers, staff can quickly lock their computer by pressing Windows Key + L.

5. Printing and Photocopying

Documents containing confidential, personal or sensitive information should be collected from printers and photocopiers promptly.

Staff should check printers, photocopiers and scanners after use to ensure that original documents or copies have not been left behind.

Incorrect or unwanted copies containing sensitive information must be disposed of through confidential waste.

6. Meeting Rooms and Shared Areas

Following meetings, staff should ensure that Council papers, handwritten notes and other documents containing sensitive information are removed from the room or disposed of appropriately.

Whiteboards and other displays containing confidential or sensitive information should be erased when they are no longer required.

Particular care should be taken in areas accessible to members of the public, contractors or external visitors.

7. Personal and Confidential Information

Additional care must be taken with information relating to employees, councillors, members of the public, suppliers and other individuals.

Examples include:

- Contact details and correspondence
- Financial and banking information
- Personnel and HR records
- Payroll information
- Complaints and casework
- Applications and personal forms
- Information relating to confidential Council business
- Passwords and system access information

Such information should only be accessible to those who have a legitimate requirement to use it.

8. Working from Home and Other Locations

The principles of this policy also apply when Council work is undertaken away from Council premises.

Council documents and devices should be positioned and stored so that information cannot reasonably be accessed or viewed by unauthorised individuals.

Council paperwork should not be left unattended in public places or vehicles unless appropriately secured.

Confidential Council information must be disposed of using an approved secure method and should not be placed in domestic recycling or household waste.

9. End-of-Day Check

Before leaving work, staff should take a brief moment to ensure that:

- Sensitive paperwork has been securely stored.
- Confidential waste has been disposed of appropriately.
- Council keys and security items are secure.
- No confidential documents have been left at printers or photocopiers.
- Computers and other devices have been locked, logged out or shut down as appropriate.
- The workspace has been left tidy for the following working day.

10. Responsibilities

All staff are responsible for following this policy and taking reasonable precautions to protect Council information.

Managers are responsible for promoting good information-security practices within their teams and addressing recurring or significant concerns.

Any loss, accidental disclosure or suspected unauthorised access to personal or confidential information should be reported promptly in accordance with the Council's data protection and information security procedures.

11. Practical Application

This policy is intended to encourage proportionate and sensible information security rather than requiring staff to work at completely empty desks.

Routine working papers may remain available while being actively used. The priority is ensuring that confidential, personal or sensitive Council information is not unnecessarily exposed or left accessible to unauthorised people.