OADBY & WIGSTON BOROUGH COUNCIL

CLEAR DESK POLICY

Policy Version Number: 3.0
Policy Author: Data Protection Officer
Authorisation: Head of Law and Democracy
Date of Next Review: February 2023

Oadby & Wigston
BOROUGH COUNCIL

Contents

1.0 Introduction

Information is an asset. Like any other business asset it has a value and must be protected. Systems that enable us to store, process and communicate this information must also be protected in order to safeguard information assets. 'Information systems' is the collective term for our information and the systems we use to store process and communicate it. The practice of protecting our information systems is known as 'information security'.

This policy is part of a set of information governance policies and procedures that supports the delivery of the Information Governance Framework. It should be read in conjunction with these associated policies, in particular the Data Protection Policy.

Oadby & Wigston Borough Council is responsible for protecting the content of its documents and records, both in paper and electronic format. The Data Protection Act requires the council to keep personal information secure.

Paper records which are left on desks/workstations overnight or for long periods of time are at risk of theft, unauthorised disclosure and damage. By ensuring that users securely lock away all papers at the end of the day, when they are away at meetings and over lunchtime this risk can be reduced.

Security risks of unauthorised access to electronic records are also prevalent when PC screens are left unattended. The council's IT system automatically locks down unused workstations after 15 minutes; however if users did this as they left their desk, the risk would be reduced still further.

Clear desks and clear screens also ensure that the council projects a professional and efficient image to visitors, members of the public and colleagues. With new ways of working such as hot-desking and working from home, it will become even more important that these issues are addressed.

2.0 Scope

This policy applies to everyone who has access to the council's information, information assets or IT equipment. These people are referred to as 'users' in this policy. This may include, but is not limited to employees of the council, members of the council, temporary workers, partners and contractual third parties.

All those who use or have access to council information must understand and adopt this policy and are responsible for ensuring the security of the council's information systems and the information that they use or handle.

This policy applies to all users whether office based or working remotely.

The policy sets out Oadby & Wigston Borough Council's requirements for each member of staff to protect any documents or records which are kept at their desk/workstation either temporarily or permanently and covers records in all formats including:

- Paper
- Electronic documents
- Emails
- Visual images such as work related photographs
- Microform including microfiche and microfilm
- Audio and video tapes, CDs, DVDs and cassettes
- Encrypted memory sticks
- Databases

This policy will also apply to any documents created in different formats in the future.

3.0 Purpose/Objectives

The purpose of this policy is to ensure users have an awareness of the importance of keeping both paper and electronic documents and records safe when they are working at their desk/workstation or on their screen and that they have knowledge of how to protect them.

It is necessary to set out such a policy to ensure:

- The confidentiality, integrity and availability of information is adequately protected.
- A reduction in the risk of security breaches through theft of paper records or unauthorised access to paper records.
- A reduction in the risk of security breaches through unauthorised access to electronic records.
- A reduction in the risk of damage to paper records by fire or malicious damage.
- The presentation of a professional image of the council to visitors, members of the public and colleagues.
- Compliance with GDPR and the Data Protection Act 2018
- Compliance with Common law duty of confidentiality.

4.0 Policy Statement

<u>Clear Desk</u>

- All users are to leave their desk/workstation paper free at the end of the day.
- All users are to tidy away all documents when they are away from their desk/workstation for more than a short period of time, namely at lunchtime, when attending meetings and overnight.
- Consideration should be given to the protective marking and sensitivity of information when storing it and this should be in accordance with the Protective Marking and Asset Control Policy.
- Documents which are likely to be needed by other members of staff should be stored in shared, locked filing cabinets.
- Other documents may be locked in storage the Council provides individual staff members.
- All office managers will have spare keys for all desks/workstations so that documents can be accessed if the staff member is absent from work.
- Users should make sure that any documents lying on their desk/workstation are not visible to visitors, members of the public or colleagues who are not authorised to see them.
- Sensitive information, when printed, should be cleared from printers immediately.

Clear Screen

- All users are expected to log off from their PCs/ laptops when left for long periods and overnight.
- When leaving their desk for lunch or to attend a meeting, users should lock down their screen using Ctrl, Alt, Del and then selecting Lock Workstation. The council's IT system does this automatically after 15 minutes, however taking this measure will reduce any security risk even further.
- Mobile devices through which access to the network can be obtained, for example PDAs, should be PIN protected, set to power off after a period of 2 minutes and switched off when left unattended. These devices should be stored securely when not in use.
- Users should make sure that no open documents on their computer screens are visible to visitors, members of the public or colleagues who are not authorised to view them.

5.0 Legislative Context

Information governance sits within a legislative background and a number of Acts of Parliament and international standards influence this policy. Users of council information systems must be familiar with the relevant legislation relating to Information Governance and Data Protection, and must be aware of their responsibilities under this legislation. Further

information about the statutory legislation governing aspects of the council's information governance arrangements can be found by contacting the Data Protection Officer.

It should be noted that in some circumstances, instances of misuse may constitute a criminal offence.

6.0 Roles and Responsibilities

It is important that all users (as defined in the scope of this policy) understand what is required of them and comply with this policy. All users are responsible for ensuring the information on their desk/workstation or screen is adequately protected in compliance with all relevant Council policies and procedures.

7.0 Training

This Policy is part of the corporate Information Governance Framework.

Appropriate training will be made available to all Council personnel.

All users will be made aware of their obligations for information governance through effective communication programmes. Each new employee will be made aware of their obligations for information governance during an induction-training programme.

Training requirements will be reviewed on a regular basis to take account of the needs of the individual, and to ensure that users are adequately trained.

8.0 Policy Compliance and Audit

Failure to observe the standards set out in this policy may be regarded as serious and any breach may render an employee liable to action under the council's Disciplinary procedure, which may include dismissal. The Disciplinary procedure is part of the Local Conditions of Employment.

Non-compliance with this policy could have a significant effect on the efficient operation of the council and may result in financial loss and an inability to provide necessary services to our customers. The council will audit its information governance procedures and where

practical and proportional, ICT Services will monitor users' access to information for the purpose of detecting breaches of this policy and/or other council policies and procedures.

It is the duty of all users to report, as soon as practicably possible, any actual or suspected breaches in information security in accordance with the Council Data Protection Policy.

Any user who does not understand the implications of this policy or how it may apply to them, should seek advice from their immediate line manager

9.0 Equality Impact Assessment

Equality and diversity issues have been considered in respect of this policy and it has been assessed that a full Equality Impact Assessment is not required as there will be no adverse impact on any particular group.

10.0 Policy Review and Maintenance

This policy will be reviewed annually, or as appropriate and in response to changes to legislation or council policies, technology, increased risks and new vulnerabilities or in response to security incidents.

Appendix 1: Policy Overview and Key Messages

Policy Overview

The overall purpose of this policy is to ensure users have an awareness of the importance of keeping both paper and electronic documents and records safe when they are working at their desk/workstation or on their screen and that they have knowledge of how to protect them.

This policy applies to everyone who has access to the council's information, information assets or IT equipment, whether office based or working remotely.

Key Messages

Clear Desk:

- All users are to leave their desk/workstation paper free at the end of the day.
- All users are to tidy away all documents when they are away from their desk/workstation for more than a short period of time, namely at lunchtime, when attending meetings and overnight.
- Consideration should be given to the protective marking and sensitivity of information when storing it and this should be in accordance with the Protective Marking and Asset Control Policy.
- Documents which are likely to be needed by other members of staff should be stored in shared, locked filing cabinets.
- Other documents may be locked in storage the Council provides individual staff members.
- All office managers will have spare keys for all desks/workstations so that documents can be accessed if the staff member is absent from work.
- Users should make sure that any documents lying on their desk/workstation are not visible to visitors, members of the public or colleagues who are not authorised to see them.
- Sensitive information, when printed, should be cleared from printers immediately.

Clear Screen:

- All users are expected to log off from their PCs/ laptops when left for long periods and overnight.
- When leaving their desk for lunch or to attend a meeting, users should lock down their screen using Ctrl, Alt, Del and then selecting Lock Workstation. The council's IT system does this automatically after 15 minutes, however taking this measure will reduce any security risk even further.

- Mobile devices through which access to the network can be obtained, for example PDAs, should be PIN protected, set to power off after a period of 2 minutes and switched off when left unattended. These devices should be stored securely when not in use.
- Users should make sure that no open documents on their computer screens are visible to visitors, members of the public or colleagues who are not authorised to view them.