Information Security Document

Secure Desk Policy

Version 9.0

Version History			
Version	**Date**	**Detail**	**Author**
1.0	20/12/2011	Completed for distribution	Mary McElvaney
1.0	25/01/2012	Approved by Information Governance Group	Jo White
2.0	27/02/2013	Reviewed by Information Governance Group	Jo White
3.0	11/03/2014	Reviewed by Information Governance Group	Jo White
4.0	13/04/2015	Reviewed by Information Governance Group. Information changed to data. Bullet point about scanning added.	Jo White
5.0	09/05/2016	Reviewed by Information Governance Group.	Jo White
6.0	09/05/2017	Reviewed by Information Governance Group. Confidential Waste procedures updated.	Jo White
7.0	11/06/2018	Reviewed by Information Governance Group. DPA 2018 and special categories of data added.	Jo White
8.0	08/07/2019	Reviewed by Information Governance Group. No changes.	Jo White
9.0	14/07/2020	Reviewed by Information Governance Group. Additions of staff working remotely. Frequent changing of keypads added.	Jo White

This document has been prepared using the following ISO27001:2013 standard controls as reference:

ISO Control	Description
A.6.1.1	Information security roles and responsibilities
A.9.3.1	Use of secret authentication information
A.11.2.8	Unattended user equipment
A.11.2.9	Clear desk clear screen policy
A.16.1.2	Reporting information security events
A.18.1.4	Privacy and protection of personally identifiable information

1 Introduction

Information, in whatever form it takes, is a valuable asset to the organisation and consequently needs to be suitably protected. Protecting information is not only a corporate responsibility; it is also a responsibility which all staff including Elected Members, partners, vendors and contractors, working in or for Derbyshire County Council must take seriously.

The Secure Desk Policy supports the Information Security Policy and other related policies such as the Safe Haven Guidance.

2 Objectives

The objective of this policy is to ensure that all paper and electronic records containing person identifiable information, or any other confidential/sensitive information (including corporate or commercially sensitive information) is suitably secured when not in use and is not left visible on an unattended desk.

This policy applies in particular to working areas, such as desks or tables, which should not have confidential, sensitive, commercially sensitive or person-identifiable information left on them whilst unattended for an extended period.

The objective of this policy is also to ensure that the Council adheres to the obligations placed upon it by the Data Protection Act 2018 as well adhering to the Derbyshire County Council Code of Conduct and the Safe Haven Guidance.

3 Key Principles

The key principles of adhering to the Secure Desk Policy are listed below:

- To reduce the risk of a security breach or information theft;
- To reduce the risk of confidential or sensitive information / documentation being stolen or accessed by unauthorised individuals which could damage the integrity of Derbyshire County Council;
- To help demonstrate compliance with the Data Protection Act 2018;
- To create a culture of staff responsibility in relation to the handling and care of personal data and other confidential information;

3.1 Definitions

Personal Data

Personal data is information which can identify a living individual – in which the person is the focus of the information and which links that individual to details which would be regarded as private e.g. name, private address, home telephone number, National Insurance number etc.

For example this could include printed spreadsheets of staff and payroll details or address files.

Special Categories of data

Special Categories of data is where the personal data contains details such as that person's:

- Race/ethnic origin
- Political opinions
- Religious or philosophical beliefs
- TU membership
- The processing of generic data
- The processing of biometric data for the purposes of identifying a natural person
- Data concerning health
- Data concerning a natural person's sex life or sexual orientation

Personal data can also include information relating to criminal convictions and offences.

For this type of information even more stringent measures should be employed to ensure that the data remains secure.

Corporately and commercially sensitive information

Corporately and commercially sensitive information may, through improper disclosure, cause reduced competitiveness or breach procurement practices. Such information may include building leases, commercial / third party contracts or internal plans.

4 Scope

It is the responsibility of those listed below to ensure they adhere to the Secure Desk Policy across Derbyshire County Council and where staff are working from home or remote sites.

- All Council employees
- All contractors and vendors
- All elected members
- All partner agencies using Derbyshire County Council premises
- All visitors using the "hot desk areas"

The policy applies to all staff in all the organisation's locations, irrespective of area of work or discipline.

The policy applies to desks, tables, computer screens, photocopier, fax and printer areas.

5 Responsibilities

- All employees, contractors, elected members, vendors, volunteers and agency staff are required to comply with the Secure Desk Policy within the office and whilst working remotely, including homeworking.
- Line managers are responsible for monitoring compliance and providing guidance to staff on the implementation of the policy.
- All employees, elected members, contractors and agency staff have a responsibility to report security incidents and breaches of this policy as quickly as possible via the Council's Incident Reporting Procedure.

The Council will take appropriate measures to remedy any breach of the Secure Desk Policy through the relevant framework in place. In the case of an employee, then the matter may be dealt with under the Council's disciplinary process. Internal reviews by management and Internal Audit, including spot checks will take place in order to identify potential breaches of this policy.

6 SECURE DESK PROCEDURE - PROTECTING INFORMATION

Confidential or sensitive information, whether held electronically or on paper records and other valuable resources should be secured appropriately when staff are absent from their workplace and at the end of each working day.

To facilitate this, the following guiding principles have been produced which cover both non-electronic (e.g. manual/paper files) as well as electronic forms of information.

In addition reference is made to the display of information on the computer / laptop screen as well as to the security of personal property.

- Desks must be cleared at the end of each working day of any confidential or person identifiable information. Files containing confidential information must be locked securely in desks, filing cabinets or designated secure rooms at all times, other than when being used by staff. Keypads to secure rooms should be changed periodically and keys used to lock desks and cupboards should be held securely to prevent unauthorised access. All efforts must be made to keep this information secure and not readily accessible to non-authorised staff. □

- To reduce the risk of a breach of confidentiality and adherence to the Data Protection Act, when disposing of person identifiable information, ensure that it is destroyed securely using approved methods of waste disposal. (See Confidential Waste Policy).

- Personal items (i.e. keys, handbags, wallets etc) should be locked away safely in the interests of security. It is the responsibility of the owner to ensure all security precautions are taken.

- Health & Safety – desks and other work spaces should be sufficiently tidy at the end of each working day to permit the authority's cleaning staff to perform their duties.

6.1 Electronic Storage Devices

For the purposes of this policy electronic data and equipment will **not** be treated differently from manual records and equipment, if they contain the same type of confidential, sensitive and/or personal information. Computing and all other equipment containing data will therefore be treated with the same level of security as paper based resources.

- To ensure the security of information held electronically, lock away portable computing devices such as Laptops, tablets or other devices when not in use and it is appropriate to do so;

- To ensure the security of information held on mass storage devices such as CDROM, DVDs or USB drives, lock these away in a secure drawer at the end of the working day;

- USB drives and other such items must be locked away even if they are encrypted.

6.2 Personal Computers, Laptops and Personal Digital Assistants (PDAs)

- Computers and laptops must not be left logged on when unattended. When staff have to leave their desks for any reason, they must lock the computer by using the 'Control, Alt, Del' keys simultaneously or by pressing the 'Windows' key and the letter 'L'. Access to the computer/laptop must be protected by passwords, in line with the Safe Haven Guidance and Password Policy.

- As far as practicable, when sensitive or confidential information is being worked on, office/home screens must be closed or minimised, or the computer locked when unauthorised persons are in close proximity to the screen.

- If sensitive or confidential information is visible to an unauthorised person standing in close proximity to computer/laptop screen, they could be asked to move away to protect the confidentiality of this information.

6.3 Printers, Photocopiers and Fax Machines

- Where there is a shared printer or multi-functional device available, all printing should be locked by default, requiring the users to enter a 4 digit PIN to release their documents.

- To avoid accidentally printing to an unintended network device, computer users should additionally check that their default printer is correct before printing any documents.

- Where documents are scanned using photocopiers or multi-functional devices, ensure that scanned documents are correctly rooted to the 'owner' of the document and then accurately filed to a secure network drive or EDRM folder structure.

- Personal data must be cleared from printers, photocopiers and fax machines immediately on completion. If these are no longer required the items must be shredded or sent for secure disposal.

- It is the responsibility of the person who sends information to be printed to ensure they collect their documents. All documents should be sent to print using the locked print facility. If information is of a confidential/sensitive nature and it is misplaced or missing, this should be logged as an incident via Service Desk online.

7 Breaches of Policy

Breaches of this policy and/or security incidents can be defined as events which could have, or have resulted in, loss or damage to Council assets, or an event which is in breach of the Council's security procedures and policies.
All employees, elected members, partner agencies, contractors, volunteers and vendors have a responsibility to report security incidents and breaches of this policy as quickly as possible through the Council's Incident Reporting Procedure. This obligation also extends to any external organisation contracted to support or access the Information Systems of the Council.

In the case of third party vendors, consultants or contractors, non-compliance could result in the immediate removal of access to the system. If damage or compromise of the Council's ICT systems or network results from the non-compliance, the Council will consider legal action against the third party. The Council will take appropriate measures to remedy any breach of the policy through the relevant frameworks in place. In the case of an individual the matter may be dealt with under the disciplinary process.

8 References

The organisation shall comply with the following legislation and other legislation as appropriate:

- The Data Protection Act (2018)
- The Data Protection (Processing of Sensitive Personal Data) Order 2000.
- The Computer Misuse Act (1990)
- The Health and Safety at Work Act (1974)
- Human Rights Act (1998)
- Regulation of Investigatory Powers Act 2000
- Freedom of Information Act 2000
- Health & Social Care Act 2001 and 2012
- Caldicott Guidelines

Organisation Policies supporting the Secure Desk Policy:

- Information Security Policy

- Information Governance Policy
- Confidentiality and Data Protection Policy
- ICT Acceptable Use Policy
- Internet, Email and Social Media Acceptable Use Policy
- Network Security Policy
- Information Risk Management Policy
- Corporate Records Management Policy
- Derbyshire Safe Haven Guidance
- Confidential Waste Procedures
- Disciplinary Policy and Procedure
- Password Policy

This document is owned by the Information Governance Group and forms part of the Council's ISMS Policy and as such, must be fully complied with.