Cotmanhay Infant and Nursery School	**Information Security Policy** **Secure Desk Policy**		
	☐ **Complete Revision** ☒ **Partial Revision** ☐ **New** ☐ **No changes**	**Review cycle:** **3 years**	**Pages:** **6**

Author of the policy:

☐ **Derbyshire County Council**	☒ **School based**	☐ **Other**
	Name: Kerry Gillott	Details:

If Derbyshire County Council / DfE, which issue number: N/A

Issue 1	Issue 2	Issue 3	Issue 4	Issue 5	Issue 6	Issue 7	Issue 8	Issue 9	Issue 10

REVISION RECORD:

Review date	Revised by	Comments
13.12.2020	KG	Change of Date
6.10.2023	KG / SM	Importance of locking computers and ipads when leaving the device. (highlighted) Few changes

We are committed to safeguarding and promoting the welfare of children and young people and expect all staff and volunteers to share this commitment.

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.

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 school adheres to the obligations placed upon it by the Data Protection Act 1998 and GDPR 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 the school;
- To help demonstrate compliance with the Data Protection Act 1998;
- 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, photographs, login codes etc.

Sensitive personal data

Sensitive personal data is where the personal data contains details such as that person's:

- Physical or mental health condition
- Sexual life
- Ethnic origin
- Religious beliefs
- Political views
- Criminal convictions
- Membership of a trade union

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. Staff sign a declaration of pecuniary and personal interest form annually.

4 Scope

It is the responsibility of those listed below to ensure they adhere to the Secure Desk Policy across Derbyshire County Council

- All school employees
- All contractors and vendors
- All governing body members
- All partner agencies using school premises

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 and agency staff are required to comply with the Secure Desk Policy.
- 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 to the Headteacher.

The school will take appropriate measures to remedy any breach of the Secure Desk Policy. In the case of an employee, then the matter may be dealt with under the 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. All efforts must be made to keep this information secure and not readily accessible to non-authorised staff. All areas are compliance checked for GDPR annually.

- 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. There is a end of employment check that is carried out by members of staff to ensure data is removed from the system.
- 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 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 or devices when not in use and where appropriate*;*

- To ensure the security of information held on mass storage devices such as 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 , devices

- 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.
- As far as possible, when sensitive or confidential information is being worked on, the window 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 and Photocopiers

- 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 folder structure.

- Personal data must be cleared from printers and photocopiers immediately on completion. If these are no longer required the items must be shredded or sent for secure disposal. If an item is printed in error staff members know to place in the secure file located near the printer.

- **It is the responsibility of the person who sends information to be printed to ensure they collect their documents.** If information is of a confidential/sensitive nature and it is misplaced or missing, this should be logged as an incident with the Data Compliance Manager or Headteacher.

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 school assets, or an event which is in breach of the school'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

School's Incident Reporting Procedure. This obligation also extends to any external organisation contracted to support or access the Information Systems of the School.

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 School'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 (1998)
- GDPR 2019
- 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
- Confidentiality and Data Protection Policy
- ICT Acceptable Use Policy
- Internet and Email Acceptable Use Policy
- Network Security Procedures
- Information Risk Management Policy
- Records Management Policy
- Safe Haven Guidance
- Disciplinary Policy and Procedure
- KCSIE updated 2023

This document must be fully complied with.

Data will be processed in line with the requirements and protections set out in the General Data Protection Regulation.

Review: October 2026