Secure Desk Policy

Public | GDPR

Version 3.0 | Published 16th July 2019 | Owner: DPO | Next Review: August 2020

Contents

1. Introduction

Information, in whatever form it takes, is a valuable asset to the Trust and consequently needs to be suitably protected. Protecting information is not only a corporate responsibility; it is also a responsibility which all Trust employees, Volunteers, Trustees, Local Governing Committees, Partners, Service Providers and contractors, working in or for Cidari Education Limited must take seriously.

The Secure Desk Policy supports safeguarding, confidentiality, GDPR, data protection and other related policies.

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 Cidari Education Limited adheres to the obligations placed upon it by the General Data Protection Regulation (GDPR) (EU) 2016/679.

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 Cidari Education Limited;
- To help demonstrate compliance with the General Data Protection Regulation (GDPR) (EU) 2016/679.
- 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.

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.

4. Scope

It is the responsibility of those listed below to ensure they adhere to the Secure Desk Policy across the Cidari family.

- All Cidari employees
- All Volunteers
- All contractors and vendors
- All Governing Committees
- All Board Members
- All partner agencies using Cidari 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, volunteers, contractors, Board Members, Governors 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, Board Members, Governors, contractors and agency staff have a responsibility to report security incidents and breaches of this policy as quickly as possible to the Data Protection Officer by emailing dpo@cidari.co.uk.

Cidari Education Limited 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 agreed disciplinary processes.

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 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 or visitors.
- To reduce the risk of a breach of confidentiality and adherence to GDPR, when disposing of person identifiable information, ensure that it is destroyed securely using approved methods of waste disposal with reference to the Trust retention schedule.
- 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 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 tablet devices when not in use and where appropriate;
- 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 and portable drives must be encrypted and must be locked away even if they are encrypted.

6.2 Personal Computers, Laptops and Tablets

- 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 'windows + L' keys simultaneously. Access to the computer/laptop must be protected by passwords, in line with the ICT user agreement and Password Policy.

- As far as practicable, 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, Photocopiers and Fax Machines

- Where there is a shared printer or multi-functional device available, print release and management solutions should be in place.
- 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.
- 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 unless required under the Trust retention schedule.
- 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 a data breach immediately with the DPO by emailing dpo@cidari.co.uk.

7. References

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

- The General Data Protection Regulation (GDPR) (EU) 2016/679.
- 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

8. Links with other policies

- Data Protection Policy
- Retention Schedule
- GDPR related documents including Privacy Notices and consents.
- ICT Acceptable Use Policy
- Internet and Email Acceptable Use Policy
- Confidential Waste Policy (pending)
- Disciplinary Policy and Procedure
- Password Policy