



Neatishead & Salhouse Federation

Clear Desk & Screen Policy

[Version 2018 v1.0]

Document version control

Version	Author	Date	Approved by	Effective from
1.0 model	DPE – JK	1/7/2018	QA -TK	May 2019

Contents

Introduction..... 4

 The need for a clear desk and screen policy 4

Key data processing principles that this policy supports... 4

Scope..... 5

Who 5

Related policies and pre-requisites..... 5

Policy..... 6

 School commitments..... 6

 Clear desk policy 6

 Clear screen policy..... 7

Additional directives by area: 8

 Reception areas and corridors 8

 Classrooms 8

 Rooms used for meetings..... 8

 Staff room..... 8

Training/Awareness 8

Audit / Monitoring / Reporting / Review..... 9

Introduction

The need for a clear desk and screen policy






The purpose of this policy is to secure information to support the Data Protection Policy and Information Security procedures.

Under the GDPR and the Data Protection Act 2018, [Our School] has an obligation to implement technological and organisational measures to show we have considered and integrated data protection into our data processing activities.

“Measures should ensure an appropriate level of security, including confidentiality, taking into account the state of the art and the costs of implementation in relation to the risks and the nature of the personal data to be protected.”

This clear desk and screen policy establishes the minimum requirements for maintaining clear work areas to mitigate the risk of information loss, theft, fraud, or a data security breach caused by personal information being left unattended and visible in plain view.

It also promotes best practices relating to information management – classification, secure storage and retention/disposal - that will support data subject rights and data processing principles.

<i>Key data processing principles that this policy supports...</i>	
Lawfulness, fairness and transparency	-
Purpose Limitation	-
Data minimisation (e.g. Sense checks for what data is really needed)	
Accuracy (e.g. Cleansing and updating/disposal of old documents and files)	
Storage Limitation (e.g. Safe disposal when information is no longer needed)	
Security: Confidentiality, Integrity, Availability (e.g. Keeping data out of site)	
Accountability of the Data Controller	

Scope

Production of a clear desk and screen policy based on data management and classification best practice for school records, devices or applications deployed in support of school and school governance activities, wherever these may be - including, but not limited to:

- IT equipment/monitors and other devices;
- Work areas including: desks/tables and storage in reception areas, offices, classrooms, staff rooms, meeting rooms, medical room and other places where personal/sensitive data may be stored or in use during the day.

Who

This policy is applicable to all staff including managers, contractors and volunteers.

Related policies and pre-requisites

This policy is to be used in conjunction with other policies such as:

- Data protection and information security policies;
- Information classification policy
In order for a clean desk policy to be effective, information management principles need to be in place to enable prioritisation of security for certain information assets following an agreed information classification such as:
 - PUBLIC e.g. curriculum information, does not warrant special security;
 - PRIVATE e.g. may include personal information, should not be on display/left out;
 - CONFIDENTIAL e.g. may include sensitive information, requires locked storage;
- Retention policy
When disposing of documents that are not duplicates of information held elsewhere, checks should be made against the school's retention policy. This may be based on the www.irms.org.uk guide:
[Information Management Toolkit for Schools](#) (see table pp37-56).

Policy

School commitments

This clear desk and screen policy will support Neatishead & Salhouse Federation in its commitment to preserving the confidentiality, integrity and availability of all pupil, staff and school-related data and information that is manually handled on paper/sticky notes, in paper-based filing systems and on IT systems or digital devices.

This clear desk policy supports Neatishead & Salhouse Federation in its commitment to the wellbeing of its staff by reducing stress and health/safety risks associated with cluttered and disorganised working environments.

This clear desk policy does not prohibit decorative personal items being left in work areas, but items of value such as purse/wallets or mobile devices should not be left out at risk of loss/theft.

Clear desk policy

Expectations of all staff, including e.g. managers, contractors and volunteers, with regard to the information and work areas they use/have responsibility for.

Documents/files and other media that include sensitive information, or those classified as confidential, shall be secured/locked away whenever they are not in use.

Desks and other work surfaces shall be left clear and tidy at the end of the working day, or when leaving a work area for extended periods, with paper work and digital devices secured, filed or disposed of as appropriate:

- All paper, documents or media that include personal or sensitive information, or that are classed as private/confidential, shall be stored in secure/lockable storage as available (desk drawers, filing cabinets, cupboards);
- Other documents shall be filed away as appropriate;
- Information that is no longer needed, in either paper or electronic form, shall be securely disposed of, or archived, in line with [The School's] retention policy.

Personal and sensitive information, or that classified as private or confidential, shall not be left unattended for any length of time without taking precautions as appropriate:

- Information shall be removed from view;
- Internal doors shall be locked if the work area is left unoccupied;
- Private/confidential information shall be secured/locked away, even if the room is locked, if others with access to the area do not have authorisation to view it.

Cupboards, filing cabinets and desk pedestals holding private or confidential information shall be kept locked by default and always when working areas are unattended and at the end of the working day.

All internal doors shall be closed/locked when working areas are unattended and at the end of the working day, and windows also closed/locked.

Keys/access control devices used for access to private/confidential information shall not be left in or near the lock or at an unattended desk.

Passwords and other security codes/encryption keys shall not be left on sticky notes posted on or under a computer, nor written down in another nearby, accessible location.

All laptops shall be secured in suitable containers when working areas are unattended and at the end of the working day.

All mass storage devices such as CD-ROMs, DVDs or USB drives [if permitted] shall be treated as 'confidential' and as such stored in a locked drawer, cabinet or store room.

All printers, photocopiers and fax machines shall be cleared of printed material as soon as they are used to ensure private and confidential documents are not left in trays/on scanners for the wrong person to pick up.

The clear desk policy shall encourage disposal of all documents no longer needed. Personal and sensitive documents should be shredded using a suitable shredder or placed in locked confidential waste bins.

Clear screen policy

Computer workstation/laptop screens shall be locked when left unattended and the device switched off/secured at the end of the working day.

PC/Laptop screens shall be positioned so they cannot be viewed by visitors in e.g. the waiting or sign-in areas and locked when not in use.

Screens shall be cleared or locked when talking to unauthorised persons.

All computer terminals shall have the auto screen saver set to activate when there is no activity for a period suggested as no longer than 15 minutes, or 5 minutes if users have access to confidential information. (Exception – see classrooms section.)

Additional directives by area:

Reception areas and corridors

Sign-in forms for day-to-day use or for open evening shall never be left out unattended.

Personal and sensitive information, or that classified as private or confidential, shall be kept in folders and securely locked away at the end of the day. It shall not be visible/stored on notice-boards/displays.

Classrooms

Workstations shall not have the auto screen saver set to avoid disturbance to teaching and learning activities, but shall be locked manually, and interactive whiteboard displays turned off, when the classroom is left unattended for any length of time.

Class lists, seating plans and other personal data shall be kept in folders and stored away securely when not in use. If seating plans include sensitive information such as SEN information, these must be stored in a locked cabinet when not in use.

Open shelves and unlocked cupboards/cupboard tops can be used to neatly store exercise books and curriculum/lesson plans, except for information/files that are personal or sensitive (confidential). This shall be locked securely away at the end of the day.

Rooms used for meetings

White boards and flip charts containing private or confident information should be erased at the end of the meeting and should be kept clean at all other times.

All meeting documents shall be removed after a meeting and the waste-bin should never be used to discard meeting notes or handouts that may include names and other personal or sensitive information.

Staff room

Staff shall not leave private and confidential information, in paper or electronic form, unattended in the staff room unless they make use of the available locked storage areas.

Open staff pigeon holes shall not be used to store or disseminate sensitive (confidential) information, such as filled in application forms, pupil SEN/safeguarding information, to avoid the risk of paper work (with possibly no backup) going missing without trace.

Training/Awareness

Members of staff and other people to whom the policy applies will be made aware of the school's clean desk and screen policy and best practices:

- At their induction;
- Through GDPR/Information security training e.g. GDPR Data Protection 101 e-learning, specifically sections on clean desks and physical security in module 2;
- Through this and other relevant school policy documents;
- Through INSET/Staff reinforcement activities;
- Through posters and other booklets/resources.

Audit / Monitoring / Reporting / Review

This policy will be audited and monitored through various means including:

- Internal audits and spot checks;
- Data Protection Officer walkarounds and observation reports;
- Feedback to the policy owner.

Reports on good/poor practices will be used to inform policy reviews as scheduled. These will be at least once annually, unless performance indicators, changes to legislation or our work practices necessitate it.
