The Yare Education Trust

Clear Desk, Clear Screen Policy

September 2018

THE
YARE EDUCATION
TRUST

Clear Desk, Clear Screen Policy

This policy sets out The Yare Education Trust'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
- Audio and video, CDs, DVDs
- Memory sticks and portable hard drives
- Databases.

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 staff 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/laptop screens are left unattended.

Clear desks and clear screens also ensure that the school projects a professional and efficient image to visitors, members of the public and colleagues.

1. Responsibility

The Yare Education Trust is responsible for this policy and Headteachers are responsible for communicating the contents of this policy to all staff, ensuring it is complied with.

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

This policy applies to everyone who has access to the school's information, information assets or IT equipment. This may include, but is not limited to employees of the school, Governors, Trustees, Members, temporary workers, partners and contractual third parties. All those who use or have access to school/Trust information must understand and adopt this policy and are responsible for ensuring the security of the Trust's information systems and the information that they use or handle.

2. Purpose and Application

2.1 If you are going to be away from your desk for an extended period of time, you should ensure you have taken reasonable measures to prevent unauthorised access to confidential information.

2.2 This policy sets out the measures you are expected to take as a minimum.

2.3 This policy applies to all staff, Governors, Trustees, Members, temporary workers, partners and contractual third parties.

3. Requirements

Clear Screen

3.1 Lock your computer (ctrl-alt-delete) when you are away from your desk. If anticipating an absence of 30 minutes or more, log off or shutdown the computer. This also applies when using a laptop.

3.2 Protect screensavers with a password.

3.3 Shut your computer down completely when leaving the office for the day.

3.4 Be aware of the position of the screen on your workstation. Wherever possible, ensure that it cannot be seen by unauthorised people while in use.

3.5 Ensure that you select an appropriately located printer where you are able to retrieve your printing immediately.

Clear Desk

3.6 Keep offices as uncluttered as possible—desks should be clear of unnecessary items.

3.7 Do not leave personal confidential information for others to find. An easy way to comply with the clear desk procedure is to work with electronic documents whenever possible – “do you need to print it”?

3.8 Store confidential papers (including seating plans with EAL/SEN/PP and Health data) out of sight. Personal confidential information must be locked away when not in use and never left unattended.

All staff must leave their desk paper free at the end of the day.

3.9 Dispose of any confidential information in designated confidential waste facilities/shredders. Never put documents containing sensitive, personal or **corporate sensitive information in the general waste bins.**

3.10 All Portable Computing and Data Storage Devices such as encrypted USB data sticks, mobile phones and laptops should be placed out of sight (including whilst in a car or residential home), preferably locked away at the end of the working day.

4. Reporting Breaches

4.1 All members of staff have an obligation to report actual or potential data protection compliance failures to the school's Chief Privacy Officer. This allows the school to:

- investigate the failure and take remedial steps if necessary
- maintain a register of compliance failures
- notify the Information Commissioner's Office of any compliance failures that are material either in their own right or as part of a pattern of failures.

4.2 The Chief Privacy Officer appointed in each school will assist with any compliance failure and establish a reporting procedure.

5. Training

5.1 All staff will receive training and/or be made aware of this policy. New joiners will receive training or information as part of the induction process and further training will be provided where necessary, including where there is a substantial change in the policy or procedures.

5.2 The Chief Privacy Officer in each school will continually monitor training needs.

6. Failure to Comply

6.1 Failure to comply with any requirement of this policy may lead to disciplinary action under the Trust's procedures.