CLEAR DESK POLICY

This policy is for all contractors of Fundamental Movement Academy (FMA). As an academy that has access to sensitive and personal children's data, a clear desk policy is the best way to avoid unauthorised access to physical records. It will also protect physical records from fire/flood damage or being mis placed.

A clear desk policy involves the removal of physical records which contain sensitive personal information to a cupboard or lockable drawer. It does not mean that the desk has to be cleared of all it's contents. At the end of the day, or if the desk or said workspace is to be unsupervised at any given time, all confidential and personal data must be filed securely away in a locked cupboard, this also applies to any electronic devices, including laptops, ipads and cameras which may hold children, staff and parent personal data. All contractors MUST ensure ..

- All sensitive/confidential information in hardcopy or electronic form is secure in their work area at the end of the day and when they are expected to be gone for an extended period of time.
- Computer workstations must be shut completely down at the end of the workday.
- Any restricted or sensitive information must be removed from the desk and locked in a drawer when the desk in unoccupied and at the end of the work day.
- Filing cabinets containing restricted or sensitive information must be kept closed and locked when not in use or when not attended.
- Keys used for access to restricted or sensitive information must not be left at an unattended desk.
- Laptop/ipads/cameras must be either locked away in a drawer if it contains sensitive information.
- Passwords must not be left on sticky notes posted on/under a computer or left written down in an accessible location.
- Printouts containing restricted or sensitive documents should be immediately removed from the printer.
- Disposal of restricted and or sensitive documents should be shredded in the official shredder bins.
- Whiteboards containing restricted and or sensitive information should be erased.
- Treat mass storage devices such as USB drives as sensitive and secure them in a locked drawer.

This policy should be read in conjunction with the data protection, retention and disposal policy.

APPROVED JUNE 2020