Human Resources

Workstation Security Policy

IMS-HRD-004

Version 2.10

Kibble
EDUCATION AND CARE CENTRE

2010-03-002

Workstation Security Policy

1. Index

Workstation Security Policy

2. Purpose

The purpose of this policy is to provide guidance on workstation security for Kibble users, in order to ensure the security of information on the workstation and information the workstation may have access to.

3. Scope

This policy applies to all Kibble employees, contractors, workforce members, vendors and agents with a Kibble *(owned or personal)* workstation, laptop, PDA, and any other mobile device connected to the Kibble network.

4. Policy

Appropriate measures must be taken when using workstations to ensure the confidentiality, integrity and availability of sensitive information, and that access to sensitive information is restricted to authorised users.

4.1. Workforce members using workstations shall consider the sensitivity of the information, and minimise the possibility of unauthorised access.

4.2. Kibble will implement physical and technical safeguards for all workstations that access electronic protected information to restrict access to authorised users.

4.3. Any electronic device (personal or business) introduced to the Kibble network must first be screened by the ICT department to establish any security vulnerabilities.

4.4. Facilitating unauthorised access (Including, but not limited to: young people, visitors and Kibble Employees) to controlled sites or sensitive/restricted data using an employee logon will be considered gross misconduct and will lead to the termination of your employment.

4.5. Appropriate measures for *workstation security* include:

- Complying with all applicable password policies and procedures.
- Securing workstations (logout) prior to leaving area to prevent unauthorised access by a young person or other members of staff to access the workstation.
- Users are responsible for the safekeeping of login details; do not under any circumstances divulge this information to other members of staff or young person.
- Do not under any circumstances log onto the network on behalf of another member of staff or young person, thereby allowing them to use your account/password to access the network.
- Ensuring workstations are used for authorised business purposes only.
- Never installing unauthorised software on workstations.

- Storing all sensitive information, including information pertaining to young people, on network servers.
- Keeping food and drink away from workstations in order to avoid accidental spills.
- Securing laptops that contain sensitive information by using cable locks or locking laptops up in drawers or cabinets.
- Complying with the Anti-Virus policy.
- Ensuring workstations are left on but logged off in order to facilitate after-hours updates. Exit running applications and close open documents.

5. Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

6. Definitions

Workstations include: laptops, desktops, PDAs, authorised home workstations accessing the Kibble network.

Workforce members include: employees, volunteers, trainees, students, and other persons under the direct control of Kibble.