APPENDIX 10

Secure/Clear Desk Procedure

May 2018

1. Introduction

1.1 A secure/clear desk is essential to mitigate the risks associated with unauthorised access to Tameside Metropolitan Borough Council's (the Council) information. Applying a secure/clear desk procedure reduces the threat of a security breach as information is kept out of sight.

1.2 In order to enable employees to work in a more efficient way, the Council is moving towards a shared working environment and there may be a requirement for an employee to work in different locations or for more than one employee to use a desk or a work station. To facilitate such a change in the working environment, a secure/clear desk procedure is essential to ensure that each work space is productive and protected.

1.3 This procedure applies to all information of a personal, confidential or sensitive nature. It also takes into account any information that is accessed, viewed or stored within a shared space (i.e. main office, home or Touch Down Point).

2. Definitions

2.1 The following terms are used throughout this document and are defined as follows:

Personal information: is any personal data as defined by the Data Protection Act 2018 and EU General Data Protection Regulations (GDPR). Broadly this is information about any living individual, who could be identified from the information or any other information that is in the possession of the Council. The Council is legally responsible for the storage, protection and use of personal information held by it as governed by the Data Protection Bill 2018 and EU General Data Protection Regulations (GDPR).

Special Category information: (similar to the concept of sensitive personal data under the Data Protection Act 1998). This data is covered by Articles 6 and 9 of the General Data Protection Regulations. As it is more sensitive it needs more protection and consists of:-

- race
- ethnic origin
- politics
- religion
- trade union membership
- genetics
- biometrics (where used for ID purposes)
- health;
- sex life; or
- sexual orientation.

Protected information is any information which is;

(a) personal/special category (sensitive personal information) *or*
(b) confidential to the Council and which could have adverse consequences for the Council if it was released in an uncontrolled way.

3. Roles and Responsibilities

3.1 All employees must ensure that their work environment follows the secure/clear desk procedure.

3.2 It is the responsibility of individual services to implement this procedure and monitor work areas.

3.3 It is the responsibility of all individuals to immediately report any actual or suspected breaches in information security by following the Incident Reporting Procedure.

4. Secure/Clear Desk Procedure

4.1 The secure/clear desk procedure is required to ensure that all protected information is held securely at all times. Information identified as protected must not be left out on desks when unattended to prevent information being read by unauthorised parties.

4.2 For periods away from your desk, working papers containing protected information must be placed out of sight and, where necessary, in a locked cupboard or drawer. Information that is not protected (i.e. contains no personal, sensitive or confidential data) may be left tidily on desks.

4.3 At the end of each day, all information should be stored in locked cupboards/drawers or within a locked room. Protected information must be stored away securely and not left on view. Computer equipment must be shut down and where appropriate laptops should be taken with you.

4.4 Protected information should not be left lying on printers, photocopiers or fax machines, even if they are in a locked room. These should all be checked at the end of the working day and any papers stored securely overnight.

4.5 Whenever you leave your desk and your PC/Laptop is switched on, you should lock your computer by pressing Ctrl, Alt and Delete and then confirm that you wish to lock your workstation.

4.6 If you are working on protected information and you have a visitor to your desk who does not have a need to know that information, ensure that you lock your screen or ensure that the information is not visible to them to prevent the contents being read. Even the knowledge that a file is held on a person can be considered an information breach.

4.7 All waste paper which contains protected information must be disposed of appropriately (i.e. shredded or placed in the Blue Locked bins). Under no circumstances should this type of waste paper be thrown away in normal rubbish or recycling bins. For further information on the secure disposal of information see the Retention and Disposal Guidelines/Schedule.

4.8 Protected information should not be stored in boxes and/or folders on top of any furniture (cabinets etc). This is insecure as they can still be accessed.

4.9 When using a hot desk or touch down point, you must consider the length of time you may be away from a desk (to attend a meeting, go for lunch, etc.). It is important to think about the security of your surroundings and secure any protected information where necessary.