APPENDIX 7

Mobile and Remote Working Protocol

May 2018

1. Introduction

1.1 The Council actively encourages employees to work differently, which will often mean employees access and process information outside the office setting. However, the Council has a duty to safeguard personal and sensitive data and equipment purchased with public funds. In addition, the technology and mobility that make portable devices so useful to employees and the Council can also make them valuable prizes for thieves.

1.2 The purpose of this protocol is to recognise the risks associated with mobile and remote working and provide employees with protocols to minimise those risks.

1.3 This protocol applies to any access or use outside Council controlled premises of:

- all Council issued static and portable ICT equipment (see definitions later) and
- any information held by the Council to which an employee has access because of his or her role within the Council.

1.4 All ICT equipment provided to employees by Tameside Metropolitan Borough Council (the Council) remains the property of the Council and must be returned promptly upon request by ICT Services or by managers for audit and inspection, to enable maintenance work to be undertaken, or for removal or disposal.

2. Definitions

2.1 The following terms are referenced throughout this document and are defined as follows;

***Outside Council controlled premises*:** includes non-Council locations such as; an employee's home, premises of another organisation and public venues.

Mobile Working: Employees who have the ability to work from multiple locations. Usually accompanied by portable computing equipment, employees can utilise any work space at any given time (including home, office, customer sites, Touch Down Points etc.).

Remote Working: Employees who are able to access information or resources from a remote location. This usually applies to workers who perform their work from home or from an alternative office (e.g. Touch-down Points) on an ad-hoc basis.

Home Working: Employees who are based at home or work from home for all or part of the working week on a regular basis. This would be an agreed arrangement and would necessitate the provision of appropriate equipment, which may be static or portable.

Personal information: is any 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 such information as governed by the Data Protection Act 1998.

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 data); *or*

(b) Confidential to the Council and which could have adverse consequences for the Council if it was released in an uncontrolled way.

VPN (Virtual Private Network): refers to a secure network connection that uses the internet to transmit data. It allows employee's access to the Council network out of the office from a Council issued PC/laptop.

Netilla: works in a similar way to a standard VPN but instead of connecting the PC/laptop to the network, it enables a user to connect from any machine as a remote virtual desktop is created. This solution may be replaced be an alternative.

Wi-Fi Hotspot: wireless internet access point in a public location such as a café, retail outlet or hotel.

Personal (Wi-Fi) Hotspot: a wireless internet access point provided by a smartphone.

2.2 In this protocol the term 'portable devices' includes but is not restricted to the following:

- Laptop/slate computers;
- Personal Digital Assistants (PDA's);
- BlackBerry's/Smartphones;
- Mobile phones;
- Text pagers;
- Wireless technologies;
- Digital Cameras; and
- Storage devices including flash memory cards/USB memory sticks.

3. Roles and Responsibilities

3.1 All employees are responsible for the safety and security of portable devices issued to or used by them. Particular care must be taken when moving equipment between sites and storing when not in use.

3.2 Where the Council provides a laptop computer to an employee, it is the responsibility of the employee to ensure that the anti-virus updates are maintained by regularly connecting the device directly to the Council network. This can be done by connecting via a designated Touch-down Point or from their office within a Council building and any automatic update should be downloaded. If employees are not clear on how to check if their anti-virus files are up to date refer to the Service Portal 'how to guides' which can be accessed via the home page of the intranet.

3.3 Employees must not install any software or connect any hardware to a Council owned portable device without the prior permission of the Council. However connection to the following is permitted:

- an external monitor or projector;
- equipment supplied, owned or configured by the Council;
- internet connection via a home router or home broadband modem (wired or wirelessly connected); and
- A printer.

3.4 Employees must not update or change the security configuration of any Council ICT equipment unless advised by ICT Services. This is to prevent potential loss of protected information or damage to a portable device.

3.5 All employees with a Council issued portable device are responsible for the information held on the device. Employees must be aware of their surroundings and take appropriate

measures when viewing information on a portable device to ensure it is not within view of others.

3.6 It is the responsibility of individuals to immediately report any actual or suspected breach in information security by informing their line manager and/or the Risk and Insurance Manager. Any incident where protected information is lost, leaked or put at risk must be reported as a potential security incident. Failure to do this could not only result in reputational damage, but fines could also be imposed by the ICO. The ICO can also fine individuals.

3.7 To reduce the risk of unauthorised access whilst working out of the office, protected information must only be stored on Council issued portable devices if they are encrypted (e.g. laptops). Some items like digital cameras cannot be encrypted, however if the contents would be considered to be protected information, the camera (or other storage medium) must be kept securely until it can be transferred to a more secure storage format.

4. Council ICT Equipment and Wi-Fi

4.1 To facilitate mobile working and working differently the Council will, by default, issue one laptop or other alternative mobile device to those that need access to the Council's systems. In addition some employees will also be issued a mobile phone, which may be a smartphone, such devices will be authorised by the employee's manager on an individual basis to support the delivery of service provision. All equipment used to store or access any protected information must be supplied, configured and installed by the Council or a Council approved third party provider.

4.2 Council provided Wi-Fi is available in most main Council buildings. Staff must use the TMBC_Staff channel. Only Council owned equipment should be connected to this Wi-Fi channel. VPN will still need to be used to make the connection to the Council's network. Two other Wi-Fi channels (public and guest are available and staff owned devices should use the public channel).

4.3 Equipment supplied by the Council may only be used by authorised persons. Employees must therefore ensure that the supplied equipment is **not** used by anyone outside the Council. Access to protected information by anyone outside the Council would have to be agreed by a Service Unit Manager. There are instances where permissions may not be required, i.e. showing a Service User information being created about them. However, in this case your Manager should be aware of what you are doing.

4.4 ICT equipment may be used for personal purposes by employees so long as it is in accordance with Information Governance Conduct Policy and appropriate supporting policies, protocols, procedures and guidance documents. However, the Council owned equipment must not be used to undertake any private business enterprise.

4.5 All faults or requests for upgrades must be logged via the ICT Service Desk (available from the home page of the Staff Portal).

5. Non-Council Equipment

5.1 Personal or any other non-Council equipment must not be used to conduct official Council business. This would include employees own smartphones (including iPhones), laptops, iPads/slate PCs, personal desktop computers or internet cafes. However, employees may use remote solutions provided by the Council such as OWA (Outlook Web Application) or Netilla (this solution may be replaced). Under no circumstances should Council data be stored or downloaded onto any non-Council equipment, as it then becomes insecure.

5.2 The setting up of personal iPhones or smartphones to receive "push" emails from an employees' own Council Outlook account must **not** be undertaken. Also, Council emails must **not** be forwarded on to a personal email account. Emails sent in these ways exit the

Council's network and are transmitted over an untrusted network. If an email or attachment containing protected information is sent to a personal device/email account, the contents are open to misdirection, interception and corruption and therefore this would be in breach of this protocol.

5.3 Employees must not install any Council owned/licensed software onto personal equipment, unless this has been authorised by ICT Services. Any software purchased by the Council is licensed to the Council and any unauthorised use outside of the licence is likely to be a breach of copyright and could result in a prosecution.

5.4 Non-Council owned portable devices including mp3 players, iPods/iPhones, cameras and USB memory sticks must **not** be physically connected to Council owned equipment unless expressly authorised by ICT Services. For further information on this, refer to the Removable Media Protocol. The connection of unencrypted devices is logged and monitored by ICT and downloads to these devices are prevented.

6. Physical Security and Insurance

6.1 Portable devices issued by the Council are usually insured when they are inside the United Kingdom, although misuse or inadequate protection may invalidate that insurance cover. Employees must seek advice from the Risk and Insurance Team before taking any Council owned portable device outside the United Kingdom as the device may not be covered by the Council's normal insurance against loss or theft. There is also the possibility that the device may be confiscated by Airport Security staff, which could result in having to leave them behind, or they may request to see the contents, which could result in a breach of this policy and possibly the law if the device contains protected information.

6.2 Employees should be aware of the physical security risks associated with working from a remote office or mobile working location. All protected information (including information stored on portable devices and in paper files) must not be left where it would attract the interest of an opportunist thief. Protected information must be located securely and out of sight so that visitors or family members do not have access. Unauthorised disclosure of protected information is a breach of this protocol and the law.

6.3 Council equipment and protected information must be kept safely and securely at all times. When equipment/protected information are at home, employees must:

- ensure that only the employee has access to the equipment/information;
- ensure that the equipment/information is safely and securely locked away when not being used;
- prevent access to the Council equipment and protected information, by family members and visitors; and
- ensure that any telephone conversations discussing protected information cannot be overheard.

These precautions are necessary to reduce the risk of unauthorised persons listening to or viewing Council information.

6.4 Employees who regularly work at home must have a suitable workstation where these issues have been considered. In order to prevent a potential breach, documents should be collected from printers as soon as they are produced and not left where they can be casually read.

7. Use of Information Out of the Office

7.1 All Council supplied laptops (and all USB memory sticks authorised for use by the Council) are encrypted and so provide a secure method in which to save information when necessary. However, whilst this is likely to prevent unauthorised access to the information,

it does not protect the information against loss. Therefore documents and files should be saved on shared drives to prevent any loss of information. Master copies of information must never be held on a portable device on anything other than a temporary basis. Once the temporary information is no longer required on the portable device it must be deleted.

7.2 It is also possible to setup folders so that they can be worked on off-line, which means there is a local copy of the data. This will allow a user to work out of the office without access to the Council network. However only a limited number of folders should be made available off-line in order to avoid performance issues on the laptop. In addition folders that contain personal data should only ever be made available off-line on a temporary basis.

7.3 All Council supplied laptops are provided with software to connect to a Virtual Private (VPN) network to allow secure access to the Council Network. VPN software will NOT be installed on non-Council equipment as this is a security risk. Most employees are issued with a laptop but if you are using a static computer and you need remote access to the council network please submit a request to exchange your computer with a laptop. In some rare circumstances, information may need to be accessed via an authorised mobile device or transferred to a form of removable media to assist mobile and remote working. If the information is of a protected nature, it is essential that the media or device has been issued by the Council and is encrypted and your line manager **must** be aware of what you are doing.

7.4 When working out of the office, employees should avoid using Wi-Fi Hotspots or free Wi-Fi connections provided by retail outlets, coffee shops and the like. Even when connected via the Council's VPN, hackers could still intercept transmissions potentially revealing protected information or password and login details. Individuals are required to assess the risks based on the data they work with. Those that work with personal and sensitive data should not use such facilities and instead use the personal Wi-Fi hotspot facility on their Council provided smartphone (also using the VPN software on their laptop). Others are permitted to use these facilities but must never give any information about their Council email account or passwords. Employees must refer to their manager or the Risk and Insurance Team if they are uncertain. The only exception to this would be a private network that requires a password to access, for example Wi-Fi at another Local Authority building, or at a business or academic premises. Purchased connectivity at a hotel, where you are given a unique password would also be acceptable.

7.5 Some services may require physical documentation (e.g. paper files) to be removed from the office to assist with mobile and remote working. If this is the case, a booking out system should be in place which meets the requirements of the service. This is to ensure that your Manager is aware of the movement of information within their service, as if a loss occurs they will need to provide assurance they were controlling their information adequately.

7.6 Arrangements must be made to properly dispose of any protected information used out of the office in order to prevent unauthorised access. To do this any information that would qualify as being personal or sensitive must be returned to the Council office and disposed of in the blue Iron Mountain security bins or shredded.