APPENDIX 6

Removable Media Protocol

May 2018

1. Introduction

1.1 Tameside Metropolitan Borough Council (the Council) recognises that sometimes there is a business need for information to be temporarily stored outside of the Council's secure network. However, the Council must safeguard information against unauthorised disclosure or loss and also prevent unintended or deliberate adverse impacts to the Council's data and networks.

1.2 Note that data accessed via, or held on, a Council issued portable device is covered in the Mobile and Remote Working Protocol.

1.3 This protocol aims to ensure that the use of removable media is controlled in order to reduce the risks associated with storing information outside of the Council's secure network.

2. Definitions

2.1 Removable media refers to devices that are used to store or transport data. In this protocol the term 'removable media' includes but is not restricted to the following;

- Optical Disks (CDs, DVDs);
- USB Memory Sticks (also known as pen drives or flash drives);
- Memory Cards (including Flash Cards, Smart Cards and Mobile Phone SIM Cards);
- Media Card Readers;
- External Hard Drives;
- MP3 Players;
- Digital Cameras; and
- Magnetic/Audio Tapes (including cassettes from Dictaphones and backups).

2.2 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 the EU General Data Protection Guidelines (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 Act 2018 and the EU General Data Protection Guidelines (GDPR).

Sensitive personal information: is any personal information (as defined above) which consists of details relating to their:

- racial or ethnic origin;
- political opinions;
- religious or similar beliefs;
- mental/physical health or condition;
- sexual life;
- a committed or alleged offence; and
- details of the proceedings or the sentence of any court.

Protected Information is any information which is:

(a) personal/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.

3. Roles and Responsibilities

3.1 All those who have access to or use of removable media are responsible for the safety and security of the media and the information stored on them and must ensure they are not compromised whist under their control.

3.2 Any incident where protected information is lost, leaked or put at risk must be reported as a potential security incident. It is the responsibility of all individuals to immediately report any actual or suspected breaches in information security by informing your line manager and/or Risk and Insurance Manager. Failure to do this could result in a loss having more serious consequences than would otherwise have been the case and could result in fines by the Information Commissioner.

3.3 Service areas are responsible for implementing this procedure and must monitor the use of removable media.

4. Use of Removable Media

4.1 Removable media (and the associated software/hardware) must only be used if there is a valid business need and with the approval of a Service Unit Manager or above. Use of removable media to transport protected information outside the office environment should be minimised and used as a last resort when no other method of accessing information is available.

4.2 Employees should be aware that the use of removable media on the Council's network is logged and monitored and may be subject to audit and inspection.

4.3 Any removable media connected to the Council's network that is not encrypted will be 'read only' and no information will be able to be saved onto it. A message will be displayed by the monitoring software. Employees will still be able to view the contents of non-encrypted media.

4.4 Files on removable media are automatically scanned for viruses before opening.

4.5 As set out in the ICT Security Policy, only encrypted USB memory sticks may be used to store information for which the Council is responsible

4.6 Purchases of removable media must be done through the Council's approved ordering system. All removable media devices and any associated software must be supplied, configured and installed by authorised Council personnel or a Council approved third party provider.

5. Security of Information

5.1 Removable media must not be used as the sole storage method for business information. Information must be stored on the Council's infrastructure which is secure and appropriately backed up.

5.2 Removable media must not be used to store backup data. All data held on the Council's infrastructure is already appropriate backed up.

5.3 Information held on removable media should be a short-term measure. Where digital information is transferred it is important to remember that at the point it is transferred, it

becomes a snapshot of the information at that time. Information temporarily held on removable media should be appropriately labelled to ensure that anyone viewing the information can easily identify the version and its content.

5.4 In order to minimise physical risk such as loss or theft, all removable media must be stored in an appropriately secure and safe environment when not in use (e.g. locked cupboard or drawer).

5.5 Anyone using removable media devices must be able to demonstrate that reasonable care is taken during transportation to avoid damage or loss. Removable media should not be used if direct access to the Council network is available at the remote site.

5.6 Council issued removable media must not normally be connected to non-Council owned equipment. Exceptionally, permission may be granted by a Service Unit Manager or above if there is a strong business case for the connection. Advice from ICT Services should be taken to minimise risk of virus infection and data loss.

5.7 Passwords needed to access protected information on removable media must only be disclosed to those authorised to access the information held on the media. Passwords must **never** be written down or stored alongside the media.

6. Access to Information

6.1 Removable media issued by the Council must only be used for the purposes of Council business. Employees must therefore ensure that any removable media is not accessed by anyone outside the Council without the agreement of a Service Unit Manager.

6.2 Protected information must not be transferred to an external third party (e.g. contractor, partner) via removable media unless this is specified within a relevant Information Sharing Agreement. If removable media is to be used, the security arrangements for the media must also be recorded and reflected within the agreement.

6.3 Should third parties be granted access to Council information, the third party is required to follow this protocol when they use removable media for the purpose of holding or transferring information.

7. Secure Disposal of Removable Media

7.1 It is essential that all removable media is disposed of securely to minimise the risk of the accidental disclosure of sensitive information. For further details on this, refer to the ICT Equipment Disposal/Recycling Policy.

7.2 Tapes can be disposed of using the secure tape bins that are provided by Iron Mountain. Discs can be carefully snapped in half or shredded (if your shredder is capable) or cut into pieces.

7.3 Removable media devices associated with mobile phones (SIM cards, memory cards etc.) should be returned to Digital Tameside along with the relevant device to ensure any data is removed from the handset before reallocation/disposal.