APPENDIX 3

ICT Security Policy

May 2018

1. Introduction

1.1 ICT is an increasingly integral part of the Council's activities and is essential in the delivery of most services. Almost all Council employees and Councillors will use Council ICT in the course of their duties. This policy is designed to enable the Council to:

- Get the best return possible for the investment it has made in technology;
- Comply with the law;
- Minimise legal and other risks associated with the use of technology;
- Ensure effective running of the Council's business;
- Minimise the risk of disruption caused by computer viruses and inappropriate us of ICT; and
- Provide clear information to employees and councillors and increase the ICT skills of our employees and resident.

1.2 This policy sets out the Council's policy on using its computers and networks, including all devices such as telephones, mobile phones; faxes; printers, scanners and anything of an electronic nature otherwise referred to as information technology etc. This equipment is for clarity of understanding referred to throughout this policy as the Systems.

1.3 This policy applies to all Council employees and Members who use the Systems. It also applies to other people using the Systems such as agency workers and contractors' staff.

1.4 Where this policy says that something is not permitted without the Council's permission it means that you need the written permission of your Service Unit Manager or above or the Head of ICT Services.

1.5 The Council's Systems are the property of Tameside MBC. In order to protect the Systems, the Council reserves the right to amend any of the policies and procedures set out in this document from time to time, following due consultation with the relevant trades unions.

2. User Responsibility

2.1 All users have responsibility for the technology they use. Responsibility extends from the Service Unit Manager who oversees a complete system to individual employees with a PC/Laptop on their desk. Everyone using ICT must observe the following:

- ***Equipment Purchase/Disposal*** – all Council equipment must be purchased through ICT Services using the Agresso procurement facility. All equipment must be disposed of through ICT services to ensure that legislation is complied with both in respect of the environment and security of information. Changing hard drives; moving ICT equipment or disposing of it without taking appropriate measures to keep information secure is likely to result in confidential information becoming available to persons not entitled to the data and consequentially breaches in statute – requirements to be followed can be found in the ICT Equipment Disposal Policy
- ***Equipment Maintenance*** - if equipment malfunctions you should contact the ICT Freshdesk for advice and assistance. Employees are not permitted to attempt to repair or maintain their ICT equipment, except for day-to-day needs such as replacement ink cartridges in printers etc. Equipment must be kept clean, especially screens and keyboards, and this is the responsibility of the employees using the equipment.
- ***Accidental Damage*** - employees are expected to make efforts to avoid circumstances that may result in accidental damage, such as spilt coffee or equipment being dislodged off desks.
- ***Keep Equipment Safe and Secure*** - employees should ensure that the equipment provided is kept secure from theft. This particularly applies to portable equipment

such as laptop computers and mobile phones. . If Equipment is lost or damaged as a result of an employee's negligence then disciplinary action may be taken and the Council may take action to recover the loss from the employee concerned. Any queries about this should be referred to Risk Management and Audit Services (Insurance).

- ***Equipment Insurance*** – Laptops are insured if outside Council premises providing that they are kept secure, out of sight and locked in the boot of a vehicle whilst in transit. However, these portable items are only covered within the UK and must be secured when not in use. Any queries about this should be referred to Risk Management and Audit Services (Insurance).

3. Management of Data, Information and Software

3.1 Employees are expected to manage data in compliance with the law, particularly the law relating to data protection and freedom of information. The Information Governance Framework and supporting policies, protocols, procedures and guidance documents provide additional support, but the main principles are that employees must:

- ***Keep data accurate and up to date and retain for no longer than necessary;***
- ***Keep Data Secure; and***
- ***Keep Data Confidential***– The Council has legal duties under the Data Protection legislation and the Computer Misuse Act to protect the information that it holds. No personal information should be disclosed unless you are sure that you are permitted to do so. When sharing such information with third parties, checks should be made to ensure that third parties are registered as a data controller under the Data Protection Act 1998. Your manager or supervisor will be able to advise you in the first instance. If any employees have any further queries they should seek advice from the Council's statutory Monitoring Officer who is also the Data Protection Officer – Borough Solicitor.

4. Authorised Business Use

4.1 You may use the Systems where you have a legitimate business need to do so and the use is appropriate to your role or you are using the Systems for appropriate personal use in accordance with section 9 of this policy.

4.2 In order to ensure accountability in the use of the Systems, you must never use any computing device without the permission of the main allocated user.

4.3 Communications sent via the Systems represent the Council. Therefore, you must ensure that all messages, communications and information created by you on the Systems are professional in tone and content. The style and language of any messages, communications or information you create should be in accordance with standard business communications and any corporate formatting and style requirements.

5. Unathorised Use

5.1 You must never use the Council's Systems to:

- Create, review or transmit material that is offensive, untrue, defamatory, malicious, potentially damaging to the Council's reputation or disruptive in nature. In particular you are not permitted to use the Systems to create, review or transmit material containing inappropriate sexual references, discriminatory, harassing or threatening comments, or any other form of communication that would be deemed offensive in

nature and contrary to the Council's employment policies, specifically the Council's Equal Opportunities Policy, Bullying and Harassment Policy and the Information Governance Policy. For the avoidance of doubt this includes but is not limited to material containing nudity, racist remarks, and/or defamatory material;

- Access any part of the ICT facility beyond the facilities available from the main user menus or icons unless you have the Council's permission to do so;
- Use any software that has not been officially purchased, issued or approved;
- Copy any of the software on the Council's Computer Systems without the authorisation of the Council. Software will be audited on a regular basis;
- Alter the configuration of the Council's Systems, hardware or software, without prior authorisation by the Council's ICT Service (Please note: Use of approved end user software applications such as Microsoft Excel does not constitute alteration of configuration of Council Systems;
- Create or circulate chain letters or jokes; nor
- Play computer games.

6. Passwords and Security

6.1 You will be issued with passwords for accessing the Council's Systems. You must keep your password confidential and you should not disclose your password to anyone else unless you have been authorised to do so by the Council. You must not write down your passwords or display them where they could be seen by others. You must take care to see that people do not see you entering your password.

6.2 It is the Council's policy that passwords should, be changed at regular intervals. During the course of your employment you are likely to be responsible for creating some of your own passwords. When creating a password, you should not select a password that can easily be deduced by others; in particular, you should not use passwords which are easy to guess (e.g. the names of partner children or pets). It is advisable to use a mix of characters, e.g. 3 out of four of: upper or lower case alphabetic characters, numbers and symbols in each password. For further guidance please refer to the ICT Service Portal for Password Guidance, Click here and type 'password' in the search box.

6.3 When you have logged into any computer you should ensure that it is left securely so that no unauthorised person can access it. On Laptops/PCs you can do this by selecting control, alt, delete and using the menu to lock your computer.

6.4 Personal or confidential data belonging to or held by or on behalf of the Council or its partners must not be stored on removable media, such as USB memory sticks CDs or external hard drives without the express permission of the Council. Where such information is unavoidably stored on a memory stick, it must be encrypted so that if it is lost or stolen the data cannot be viewed and/or misused. For further information, please refer to the Removable Media Protocol.

6.5 When an employee leaves the Council, their access to computer systems and data must be deleted on the employee's last working day. It is the responsibility of the line manager to request access deletion via the ICT Freshdesk. Similarly, Managers must inform ICT Services when any employees change jobs within the Council so that systems can be amended and the user's systems access changed, as appropriate. For more information, see the Access and Security Protocol and Movers Checklist.

7. Approved / Unapproved Equipment and Software

7.1 You must not use or install any software on the Systems unless that software has been approved and issued by the Council. For example, you must not install or run software that

you have brought in from home, downloaded from the internet or other ICT Systems. This is to avoid conflicts between software, damage to Systems or breaking copyright law. The ban on installing or downloading software unless specifically authorised by the Council includes a ban on installing or downloading:

- Games
- Freeware and shareware
- Upgrades to existing software
- Demonstration versions of software
- Screensavers

7.2 You must not connect any equipment to the Council's Systems unless it belongs to the Council or you have the Council's permission.

8. Unauthorised Access or Modification of Systems

8.1 Unless you have been authorised by the Council to do so you must not, nor attempt to, modify the Council's Systems. (Please note: Use of approved end user software applications such as Microsoft Excel does not constitute modification of Council Systems.)

8.2 You must not misuse the Council's Systems by accessing information which you are not authorised to view or use, or to attempt to break ('hack') into any computer system, for example by using someone else's password.

9. Personal Use

9.1 The Council has devoted time and effort into developing the ICT Systems to assist you with your work. The Council does, however, recognise that there are times when you may want to use the Systems for non-work related purposes, and in recognising this need the Council permits you to use the Systems for personal use.

9.2 You must not use the Systems for personal use during working hours. If you work flexible hours then personal use must be at a time when you are not working and outside core time. You must not allow personal use of Systems to interfere with your day to day duties Excessive non-job related use of the Systems during contractual hours may be subject to disciplinary action.

9.3 You must not use Council software for personal use unless the terms of the licence permit this and you are responsible for checking the licensing position. Microsoft Office and Internet Explorer are licensed for personal use.

9.4 Use of the Systems should at all times be strictly in accordance with the provisions of paragraph 5.1 above. You must pay all costs associated with personal use at the Council's current rates e.g. cost of paper and telephone calls.

9.5 You are responsible for any non-business related files which are stored on your computer. If you connect your personal memory stick to any system you must carry out appropriate virus checks first.

9.6 When accessing the internet for non-work purposes you may only view web pages and download .pdf files. You may not download other files because they contain a risk of contamination by viruses and that risk is disproportionate to the benefits to the Council in allowing you access to them.

10. The Council's Rights and Obligations

10.1 The Council reserves the right to monitor all communications and information created, or transmitted on the Systems in order to protect the Council's legitimate business interests and the Systems. These include, but are not limited to, ensuring compliance with policies, detecting or preventing crime, recording evidence of business transactions and detecting viruses. You should not therefore expect communications conducted on the Council's Systems to be private and confidential.

10.2 Any information that the Council collects as a result of monitoring the use of its Systems will be processed in accordance with the Council's Data Protection and Freedom of Information Policies.

11. Viruses

11.1 Computer viruses have the potential to cause enormous damage to Systems and the data they hold, and severely affect service delivery as a result. Every effort must be made to avoid introducing viruses into the Council's Systems and equipment, and employees have a clear responsibility in this respect. Employees must ensure that ANY disk or memory stick being brought into the Council is virus checked before loading. If a PC does not have its own virus checking software then the ICT Freshdesk should be contacted

11.2 Viruses may be transmitted through E-mails and/or attachments. If anyone has any doubt about an e-mail received, especially from an unknown source, refer it to the ICT Freshdesk. Do not open any suspicious e-mail or attachment. Any employee who intentionally or negligently causes a virus to affect Council Systems is liable to disciplinary action. It is essential that all employees remain vigilant.

11.3 To prevent viruses damaging the Systems, all computer Systems must have the appropriate anti-virus software installed and this must be updated regularly. The anti-virus software should never be disabled. All files used on Council computer systems will be scanned automatically but for added security you should take due precautions when using any external device or media such as CDs, USB memory sticks and the like and satisfy yourself that they are virus free. For further information, please refer to the Removable Media Protocol.

12. Use of ICT at home or Out of the Office

12.1 The provisions of the Policy apply equally when working on Council data or equipment outside Council premises.

12.2 If employees are working from home on a regular/permanent basis then specific arrangements must be agreed with your Service Unit Manager.

12.3 Employees must not install Council owned software on their own equipment or connect Council owned equipment to their personal equipment.

12.4 The Council cannot be held liable if, for any reason, the use of personally owned equipment for Council business results in that equipment being damaged or adversely affected in any way.

12.5 Data must be kept securely. Employees must not use their own equipment to process personal data without the agreement of their Service Unit Manager, who must ensure that proper arrangements for the security of the data are made.

12.6 You must not store Council files on your personal equipment. You should use a Council memory stick, which is encrypted, to store such files when working on them at home. Care should be taken to ensure that:-

a) You do not store files on your computer; and
b) When you dispose of any ICT equipment you make sure that no Council documents have accidentally been stored on it and none are stored in any temporary folder – or you remove and destroy the computer's hard drive.

12.7 For full details on the use of ICT at home or out of the office, refer to the Mobile and Remote Working Protocol.

13. Ownership Rights

13.1 Work related information, communications or data created, received, stored or transmitted by you whilst you are employed by the Council (whether inside or outside of working hours) is and remains the property of the Council.

14. Health and Safety – Display Screen Equipment (DSE) Regulations

14.1 All employees have responsibility for Health and Safety in the workplace, and this will be reflected in the manner that ICT is used. Employees and Service Unit Managers are expected to ensure that the use of technology in their areas complies with the provisions of Health and Safety legislation. Employees and Service Unit Managers are expected to ensure that the workplace is kept tidy, and that the presence of technology in the office is not a cause for concern.

14.2 So far as the Council is concerned, an employee falls within the requirements of the Display Screen Equipment (DSE) regulations if they use equipment for continuous spells of an hour or more (on average) every day. The requirements of the DSE regulations can be found here and all employees and Managers should comply with them.

15. Back Ups

15.1 It is vital that backup procedures are in place to maintain the availability, integrity and confidentiality of data. ICT Services backup the corporate servers on a regular basis.

15.2 All employees must be aware that ICT only back up information stored on the network (shared drives). Information stored on local (C:) drives or the desktop is not backed up and would not be able to be recovered if the equipment was lost, corrupted etc. Therefore, information stored on local drives should be kept to a minimum.

15.3 Service Unit Managers are responsible for ensuring that appropriate backups are undertaken for any local drives or standalone PCs located in their service area.

16. Harassment and Abuse

16.1 The use of technology to harass and abuse others will not be tolerated. The Council has a clear and fundamental commitment to equal opportunities and the welfare of its employees, Councillors and others; and will not tolerate harassment in any form. This commitment is made explicit in the current 'Bullying and Harassment' policy. Any employee found to be using technology as a means of harassing others will be investigated and disciplinary action

will be taken as appropriate. This applies whether it is another employee, a councillor, or a member of the public who is subject to harassment or abuse.

17. Contraventions of the Policy

17.1 Local Government employees are expected to give the highest possible standard of service to the public. Employees are expected, through agreed procedures and without fear of recrimination, to bring to the attention of the Council any deficiency in the provision of service. Employees should report to the appropriate manager any impropriety or breach of procedure or misuse of Council property. The Council has a Whistle Blowing Policy in place to encourage and protect responsible employees to come forward, anonymously if they wish, to report instances of abuse of time, etc.

17.2 Employees should be aware that the Council Systems including the internal and external e-mail system may be monitored from time to time to ensure that the system is not being abused, to ensure that this code of practice is being complied with and for any other lawful purpose.

18. Disciplinary Implications

18.1 Breaches of this policy may result in disciplinary action up to and including dismissal. They may also result in you being prosecuted under Data Protection legislation and the *Computer Misuse Act 1990*, and may lead to prosecution of the Council and the individual(s) concerned and/or civil claims for damages.

18.2 Most use of ICT is by employees and the code has been written with them in mind. However, it applies equally to Councillors using Council owned ICT equipment. Mis-use of Council owned ICT equipment or software may be a breach of the statutory Code of Conduct for Councillors - in which case it may be reported to the Standards Board for England and/or the Council's Standards Committee who may impose a sanction.