APPENDIX 4

Email, Communications and Internet Acceptable Use Policy

May 2018

1 Introduction

1.1 ICT is an 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;
- gain maximum benefit from email and the internet;
- 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 use of ICT; and
- Provide clear information to employees and councillors and increase ICT skills of our employees and residents.

1.2 This policy sets out the expectations of individual's conduct and responsibilities when using the Council's email and internet facilities, including;

- Work related and personal use of email (including personal email accounts);
- Work related and personal use of the internet; and
- Work related and personal use of social media (including the posting of information on social media sites whether related or unrelated to any Council business).

1.3 This policy applies to Council employees, Members, agency workers, contractors, third parties and all partners who use the technology set out in 1.2.

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 AED of Digital Tameside.

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 Personal Use

2.1 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.

2.2 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. You must not allow personal use of systems to interfere with your day to day duties.

2.3 You must pay all costs associated with personal use at the Council's current rates e.g. cost of paper and telephone calls

2.4 You must not store personal files on Council systems as there is a cost to the public purse for such storage and backup of the same. You may however use 'Cloud' or on-line storage facilities (using your own personal account). If you connect your personal memory stick to any system you must carry out appropriate virus checks first. If your memory stick is not encrypted you will not be able to save any files to it.

2.5 When accessing the internet for non work purposes you may only view web pages and download .pdf files and images. 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. The Council's filtering system will prevent you from downloading programmes.

3 Email Use

3.1 The Council has developed its email system to facilitate effective business communication within the workplace. You are only permitted to use the email system for personal use in accordance with section 2 above – though you should be aware that all emails may be subject to monitoring and the right to send personal emails implies no confidentiality. All emails that you create should adhere to the provisions of this policy, and in particular comply with the requirements set out in this section.

3.2 Employees should treat e-mail communications with the same degree of care and professionalism as they would a letter sent out on company-headed notepaper. They should all meet ' the Chief Executive Test' namely would the Chief Executive send this email out on behalf of the Council or more importantly would this e-mail give the Chief Executive cause for concern if he saw it? E-mails should be courteous and written in a style appropriate to business communication and not in a casual or flippant tone. Careless or casual use of humour should be avoided, as it can be misinterpreted. The sending, or forwarding on, of jokes by e-mail (or as an attachment) is strictly prohibited.

3.3 The sending, or forwarding on, of curt, rude, sexually explicit, racially biased or offensive e-mails (or attachments) is strictly prohibited. Equally, employees are advised not to send e-mails in the heat of the moment. Employees should not send unsolicited, irrelevant, or inappropriate e-mail messages internally or externally, nor should they participate in chain or pyramid letters by e-mail. Furthermore, personal opinions should not be presented as if they were those of the Council.

3.4 You should not use the email system in breach of any of the Council's employment policies, particularly the Council's Equal Opportunities Policy, Bullying and Harassment Policy and Data Protection Policy. Employees must not use the e-mail system to send inappropriate messages or images via the email system (whether internally or externally). Inappropriate messages would include those, which are:

- Sexually explicit;
- Offensive (whether to the recipient or to a third);
- Potentially damaging to the Council's reputation and/or standards expected by the public;
- Defamatory;
- Discriminatory (e.g. racist or sexist); and
- Constitute harassment (see section 6).

3.5 Standard e-mail is not a suitable medium for the communication of confidential, personal, or other sensitive information unless you have been granted permission to do so by the Council; you should not send confidential information by standard email. Confidential information means all information which may be imparted in confidence or be of a confidential nature including but not limited to all information relating to the Council's business or prospective business. It is important to remember that email sent over the internet is not secure. You should not therefore send any confidential information by external email unless it is properly encrypted Email sent by GCSX (where available) is considered to be secure as is the use of Egress Switch.

3.6 Email is not a suitable medium for communication on any matter that requires dialogue or discussion and should not be used as a substitute for face-to-face communication.

3.7 E-mail is a `publication` for the purposes of the law. Any e-mail that includes information taken from another source (such as a publication or a website) may also breach copyright, for which the Council may be held responsible. Messages sent via the email system can give rise to legal action against the Council. Claims of defamation, harassment and breach of confidentiality or contract could arise from a misuse of the Systems. Email messages are disclosable in any legal action commenced against the Council relevant to the issues set out in the email. Employees should note that E-mail messages and any attachments can be used as evidence in many circumstances and may have to be disclosed under the Freedom of Information Act. You must use the Council's email disclaimer on emails along with a signature file providing contact details. Anyone found to be sending or forwarding inappropriate messages, or exposing the authority to legal action, may be subject to disciplinary action.

3.8 As with other forms of business communications, you should retain copies of the emails you send, where necessary, for an appropriate length of time. Please refer to separate guidance on this matter.

3.9 If an email message is sent to you in error, you should contact the sender. If the email message contains confidential information you must not disclose or use that confidential information. If you receive an email of this nature you should contact your immediate line manager.

3.10 You should only open emails with attachments from persons or organisations that you are familiar with. If you receive an email with an attachment from an unknown source and you are suspicious as to the nature of the communication you should forward the email to ICT Services to inspect before opening it. You should not open any emails which do not appear to relate to Council business and seem to contain jokes, graphics or images; as such emails regularly contain viruses.

3.11 Employees are permitted to send and receive personal email whilst at work (in accordance with section 2 above) but emails must not contain inappropriate content. Employees must not send or receive excessive numbers of personal emails and must not allow their Council email account to be used for commercial (non-Council) purposes. Excessive or inappropriate use of email may lead to disciplinary action and to withdrawal of some or all privilege.

4 Telecommunications

4.1 Employees are allowed to use the Council telephone system (and mobile telephones provided by the Council) for personal calls. However, where a cost is incurred employees will reimburse the Council with the cost of the call. Employees will not use telecommunications systems and equipment provided by the Council for any activity that is illegal, for harassment or abuse of others, or for personal gain. Any employee found doing so may be liable for disciplinary action.

4.2 Interception and Monitoring: This Policy has been prepared in accordance with Data Protection legislation, the Human Rights Act, and the Regulation of Investigatory Powers Act 2000. Exceptionally, the Council may monitor and/or intercept telecommunications Systems where permitted by the Regulation of Investigatory Powers Act 2000.

5 Internet Use

5.1 You may be able to access the internet from the Council's Systems. The internet may be used for legitimate business purposes or for personal use in accordance with section 2. Excessive non-job related use of the internet during the working day may be subject to disciplinary action. Internet access may be withdrawn if it is being abused. Employees should be aware that all visits to websites on the Internet are logged and monitored by software operating on the Councils web server and may be subject to audit and inspection and disclosure under the Freedom of Information Act.

5.3 You should try to ensure that you will not be infringing any copyright or related rights, by downloading the information.

5.3 You must not access, view or download any illegal or inappropriate material. In particular, you should not access, view or download any material that would constitute a breach of the Council's Equal Opportunities Policy and/or the Council's Bullying and Harassment Policy

5.4 You should note that, in order to protect its legitimate business interests and its systems, the Council monitor's internet use.

5.5 The Council has installed software to try to prevent access to inappropriate web pages. This includes pornography and illegal sites as well as gambling and racist sites. The risk of viruses and other malware also means that access to web-based email services is considered inappropriate. However the system relies on a list of banned sites and key word searches and so is not completely comprehensive. Employees are not permitted to access any site with inappropriate content and may be subject to disciplinary action if they do. Exceptionally, employees may need to access this type of site for work related purposes. If this need arises they must seek written authority to do so from the AED Digital Tameside or his Service Unit Managers; the Head of Risk Management and Audit Services or the Council's Monitoring Officer in advance.

5.6 It may, very rarely, happen that despite the protection systems, an employee accidentally visits an inappropriate site. If this happens then they must inform the AED Digital Tameside or his Service Unit Managers and the Head of Risk Management and Audit Services immediately by e-mail to avoid the possibility of being suspected of seeking to access inappropriate web pages.

5.7 Employees may use the internet to carry out their own private transactions (e.g. the purchase of books or tickets) in their own time but you may not carry out transactions, which would be viewed as inappropriate under other parts of this Policy. The Council will not accept any responsibility for any loss that you may suffer as a result of personal use of the internet. Employees are reminded that the Council does monitor internet use**.**

6 Harassment and Abuse

6.1 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 the harassment or abuse.

6.2 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.

7 Disciplinary Implications

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

7.2 Most use of ICT is by employees and the code has been written with them in mind. However, it applies equally to Councillors, contractors, agency staff and other third parties using Council owned ICT. 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.