APPENDIX 2

IT Acceptable Use Policy

Date: December 2023

Version: V1.2

APPENDIX 2

Document Version Control

Document Version Control		
Version Number	**Date**	**Approved by**
1.0	May 2018	Audit Panel
1.1	September 2021	N/a – consultation draft to IT/IG working group
1.2*	December 2023	N/a – consultation draft to Information Governance Group

*Version 1.2 of this policy now incorporates and replaces the following polices:

- Access & Security Protocol
- Removable Media Protocol
- Mobile & Remote Working Protocol
- Email, Communications and Internet Acceptable use

This is a live document effective from the issue date. It supersedes any previous versions of this document, which are now withdrawn.

APPENDIX 2

Contents

APPENDIX 2

1. INTRODUCTION

1.1. IT is an integral part of Tameside Metropolitan Borough Council's (the Council) activities and is essential in the delivery of most services. Almost all Council employees and Councillors will use Council IT equipment and systems 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, in particular Data Protection 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 IT; and
- Provide clear information to employees and councillors and increase IT skills of our employees and residents.

1.2. This policy applies to Council employees, including temporary contact staff and volunteers, Councillors, agency workers, contractors, third parties and all partners who use the Council's technology.

1.3. Where this policy says that something is not permitted without the Council's permission it means that you need the written permission of a Service Unit Manager of Digital Tameside or the Assistant Director of Digital Tameside.

1.4. In order to protect the Council's 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 trade unions.

2. PERSONAL USE

2.1. The Council recognises that there are times when you may want to use its systems and equipment for non-work related purposes, and in recognising this need the Council permits you to use them for personal use.

2.2. You must not use the systems or equipment for personal use during working hours. If you work flexible hours/flexibly then personal use must be at a time outside of your work hours.

2.3. You must not allow personal use of equipment or systems to interfere with your day to day duties. Excessive non-job related use of the Council's equipment or systems during contractual hours may be subject to disciplinary action.

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.

2.5. When accessing the internet for non-work purposes you may only view web pages. You may not download files/documents because they contain a risk of contamination by malware. The Council's filtering system should prevent you from downloading programmes.

3. EMAIL USE

3.1. Employees are only permitted to use the email system for work purposes. Corporate email should not be used to send personal emails or send emails for party political purposes or promotion of personal financial interests.

3.2. All emails may be subject to monitoring. 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.

3.3. 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 they 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.

3.4. The sending, or forwarding on, of curt, rude, sexually explicit, racially biased or offensive emails (or attachments) is strictly prohibited. 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.

3.5. 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 Policy.

3.6. 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 party)
- Potentially damaging to the Council's reputation and / or standards expected by the public
- Defamatory or libellous
- Discriminatory (e.g. racist or sexist)
- Constitute harassment (see section 12)

3.7. Care should be taken when sending confidential, personal, or other sensitive information. Emails sent between two ".gov.uk" accounts are generally deemed to be safe and do not require additional encryption, though employees are directed to check the Council's Safe to Send List prior to sending any protected information. All emails containing protected information sent to non .gov.uk recipients must be sent using Egress secure Mail. Consideration should also be given to using password protection on attachments (even where sent through Egress) for particularly sensitive information, though use of encrypted email is the minimum standard to be used.

3.8. 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. They may have to be disclosed under the

Freedom of Information Act 2000, or as part of a Subject Access Request under the Data Protection Act 2018 and UK GDPR.

3.9. The Council's email disclaimer and a corporate signature file including contact details are automatically added to emails sent from PCs/Laptops. This should not be removed. The corporate email disclaimer and corporate signature file are not automatically added to emails sent from a corporate smartphone.

3.10. As with other forms of business communications, you should retain copies of the emails you send, where necessary, for an appropriate length of time. Outlook automatically deletes emails after two years from the sent or received date in line with the Council's corporate email deletion protocol. Any emails stored on a shared drive/SharePoint must only be retained as long as is necessary and in line with the Corporate Retention Schedule.

3.11. Employees should not use the email system for the storage of documents/attachments. This content will be automatically deleted after two years in-line with the corporate email deletion protocol. Similarly, these documents are not available to others should an employee leave the Council.

3.12. If you send an email to an incorrect recipient, you should telephone the recipient immediately and ask them to 'double delete' (delete from their inbox and then delete again permanently from their deleted items folder) the email. You must also contact your immediate line manager and notify the Information Governance team by using the Information Security Incident Reporting From which is contained in the Personal Data Breach Reporting Procedure.

3.13. If an email message is sent to you in error, you should contact the sender immediately. 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 and double delete the email once the sender and your line manager are notified.

3.14. Autocomplete is an email feature that is enabled as standard. Autocomplete suggests email addresses in the To, cc or bcc fields when composing an email. These suggestions are based on the people you have previously emailed. It remains the responsibility of the individual to double check the suggested email address is correct. This feature can be disabled by the user.

3.15. 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 report this to IT Services by using the 'Report as Malicious' button within your email.

3.16. If you receive an email with an attachment from a known source, or an email you are not expecting, you should contact the source by telephone in order to confirm that the email is genuine. 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.

3.17. Employees should take care when subscribing to email newsletters or marketing campaigns. High volumes of this type of email place a strain on the Council's storage and there is a cost to the public purse for storage and backup of those emails. Consideration should be given to unsubscribing where the newsletter is no longer required for work purposes and employees can also use the block sender function in Outlook.

4. TELECOMMUNICATIONS USE

4.1. Employees are permitted to use the Council telephony system (including mobile phones) for personal calls. However, where a cost is incurred employees will be required to reimburse the Council for the full cost of the call. Excessive non-job related use of the Council's telephony system and/or mobile telephones may be subject to disciplinary action.

4.2. Employees must 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 subject to disciplinary action.

4.3. Mobile Phone Usage

4.3.1. Some employees will have use of a corporate mobile phone or a smartphone (if requested by the employee's manager based on an individual basis to support the delivery of service provision).

4.3.2. Your corporate mobile phone may be used for personal use in accordance with section 2.

4.3.3. Staff who are on the TMBC payroll may use their corporate mobile phone for personal calls and texts but this usage must be declared each month and paid via salary deduction via the "Mobile bills" function on the staff portal home page. Excess data usage (such as streaming video content) is prohibited as this cannot be declared and paid for.

4.3.4. Staff who have been issued with a corporate mobile phone but who are not on the TMBC payroll (such as agency staff) may not use their device for personal usage as the cost for this cannot be quantified or recovered.

4.3.5. The Council maintains a blacklist of apps that it does not authorise for business use and you will be prevented from downloading or accessing these on your corporate device.

4.3.6. The Council's mobile phone provider implements an 18+ policy on your device which will prevent you from accessing inappropriate web pages. This includes pornography and illegal sites, as well as gambling, payday loan and racist sites. Employees are not permitted to use their corporate smartphone to access any site with inappropriate content. Employees may be subject to disciplinary action if they attempt to search for or access sites with inappropriate content. In exceptional cases, 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 Assistant Director Digital Tameside, the Head of Risk Management and Audit Services or the Council's Monitoring Officer in advance.

4.3.7. To protect the Council's data that will be held on a corporate smartphone users must ensure the device is registered with the corporate security server/MDM. Details of how to do this will be sent to you when you first collect the device

4.3.8. Where the Council provides a smartphone to an employee, it is the responsibility of the employee to ensure the security updates that are automatically deployed to devices are promptly downloaded. This is best achieved by ensuring automatic updates are set to "on" in the device Settings Menu. The device may prompt you to connect to a wifi network or to charge it before downloading an update. You should ensure this is performed at the very earliest opportunity.

4.3.9. If your device is stolen or you lose or misplace it you must immediately notify IT Services via the IT Servicedesk. This is so that we can bar the device to ensure there is no further usage. You must also notify The Risk, Insurance and Information Governance Team by completing the data breach form so the incident can be investigated.

4.3.10. Corporate mobile phones must be returned to IT Services when you leave or no longer require the use of it. Under no circumstances should you hand ownership over to another member of staff, this could constitute a data breach.

5. INTERNET USE

5.1. The internet may be used for legitimate business purposes or for personal use in accordance with section 2. 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 2000.

5.2. 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

5.3. The Council has installed software to prevent access to inappropriate web pages. This includes pornography and illegal sites, as well as gambling, payday loan and racist sites. Employees are not permitted to access any site with inappropriate content and all internet activity is monitored, including any attempt to access or search for such sites. Employees may be subject to disciplinary action if they attempt to search for or access sites with inappropriate content. In exceptional cases, 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 Assistant Director Digital Tameside, the Head of Risk Management and Audit Services or the Council's Monitoring Officer in advance.

5.4. 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 Assistant Director Digital Tameside 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 and to enable ICT Services to block future visits.

5.5. Employees may use the internet to carry out their own private transactions (e.g. internet shopping) in their own time but you may not carry out transactions, which would be viewed as inappropriate under other parts of this Policy. Your Tameside email address is not to be used for private transactions. Please only use personal email addresses. 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. HOME, REMOTE AND MOBILE WORKING

6.1. Post-Covid, many Council employees now access and process information outside of a traditional office setting. This Policy covers all locations where an employee may work, including a corporate office location, another business location or the home.

6.2. Employees who work from anywhere outside of the council network will need to register for Multi Factor Authentication (MFA) which is a mandatory additional level of security required to gain access into the council network.

6.3. 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 locations and storing when not in use.

6.4. Where the Council provides a laptop to an employee and this device is mainly used out of the office, it is the responsibility of the employee to ensure that the anti-virus updates and software updates that are automatically deployed to devices are promptly downloaded. This is achieved by regularly connecting to the network via VPN then selecting "shut down" and waiting until the process is complete before closing the device.

6.5. Employees must take additional care when working at home to ensure that any 'Smart Home' or 'Internet of Things (IOT)' devices are not able to connect to the Council's IT equipment. Particular care should be taken around 'smart speakers' and / or 'smart assistants' (including but not limited to Amazon Alexa, Google Assistant, Siri etc.) built into devices including an employee's personal smartphone or tablet as such devices are capable of recording conversation that they pick even when they appear inactive.

6.6. All protected information (including information stored on portable devices and in paper files, including printed and handwritten documents and notes) must not be left unattended or where it would attract the interest of an opportunist thief. Protected information must be located securely and out of sight. Unauthorised disclosure of protected information is a breach of this Policy and the law.

6.7. Where Council equipment and protected information is used at home this must be kept safely and securely at all times. Employees must :

- ensure that only they have 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 data/information, by family members and visitors;
- ensure that any telephone conversations discussing protected information cannot be overheard.

6.8. Employees who work at home must have a suitable workstation where possible and the above issues must be considered.

6.9. Printed documents and/or handwritten notes which contain protected information must be disposed of appropriately. When working from a remote location (including at home), it is expected that any such paperwork is kept concealed at a minimum, and where possible is stored in a lockable cupboard or drawer, until you are able to make arrangements to securely dispose of paperwork at a Council office location. All waste paper which contains protected information must be disposed of appropriately in a Council office location by placing into the locked confidential waste bins. Under no circumstances should paperwork containing protected information be thrown away in domestic recycling or waste bins. For further information on the secure disposal of information see the Retention and Disposal Guidelines/Schedule.

6.10. 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. This applies whether working at home or in a public space.

6.11. When working out of the office, employees should avoid using Wi-Fi Hotspots or free Wi-Fi connections provided by retail outlets, coffee shops etc. 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, Insurance and Information Governance 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.

6.12. 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.

6.13. Employees must seek advice from the following services before taking any Council owned portable device outside of the United Kingdom:

- Risk and Insurance Team
  - 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.
- ICT Services (via the IT Service Desk)
  - Activity and logins to TMBC accounts from abroad are logged and investigated to ensure they do not relate to suspicious cyber criminal activity;
  - To ensure appropriate data roaming packages are included for smartphones to protect against excess charges and to make the users are aware of the additional costs

6.14. Employee's that work remotely should be based in the UK. If anyone has a requirement to work for a period of time outside the UK, this must be discussed with your manager and HR will need to authorise this.

7. PASSWORD SECURITY

7.1. Passwords are the first line of defence for the Council's IT systems and together with unique user ID's, passwords help to establish that people are who they claim to be. A poorly chosen or misused password is a security risk and may impact upon the confidentiality, integrity or availability of the Council's computers and systems.

7.2. In using the IT equipment provided to you by the Council you accept that you have read and accept the details within this policy, the IT Security Policy and the IT Corporate Password Policy.

8. STAFF LEAVERS AND INTERNAL MOVERS

8.1. Where an employee leaves the Council, the manager must follow the Leavers Checklist available via the intranet and must also log a "leaver request" through the IT Service Desk to ensure the correct system accesses are removed and the return of all equipment is arranged on the leaver's final working day.

8.2. Where employees move internally between different service areas within the Council, the manager of the team being left has responsibility for notifying IT Services. The manager must follow the Movers Checklist available via the intranet and must also log a 'movers request' through the IT Service Desk. Logging a ticket will ensure

- that IT equipment can be changed where necessary
- the employee's systems and data access can be amended as appropriate.

- the manager is aware of their responsibility to make their employee aware of the need to remove all data pertaining to their previous job role (emails, documents etc.)
- the employee is copied into the ticket and informed of their responsibilities around purging emails, files, data pertaining to their old role

8.3. The manager of the new team will log a "new starter" ticket on the IT Service Desk. The new starter ticket will ensure

- the appropriate IT equipment needed for their new employee is provided
- the appropriate system access is granted

8.4. Any access permissions for the new job role must be obtained in line with the process outlined in Section 10.

8.5. If an employee is deemed to have contravened this policy or any other policy on the Data Protection/Information Governance Framework, potentially jeopardising the availability, confidentiality or integrity of any systems or data/information, their access rights to the system or data/information will be suspended pending further review.

9. REMOVABLE MEDIA

9.1. Only by exception and where there is a valid business need, as agreed by the employees Service Unit Manager and with approval from a SUM of IT Services will permission be granted to store data/information on removable media (USB memory sticks, CDs, external hard drives). In all instances the device must be purchased by IT Services via the Council's approved purchasing system and will be encrypted so that if it is lost or stolen the data cannot be viewed and/or misused.

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

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

9.4. Any employee who has access to or use of removable media is responsible for the safety and security of the media and the data/information stored on them and must ensure they are not compromised whilst under their control.

9.5. 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.

9.6. 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.

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

9.8. 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.

9.9. Use of encrypted removable media to transport or access protected information outside of the Council's network should be minimised and used as a last resort when no other method of accessing information is available. Employees must be able to demonstrate that reasonable care is taken during transportation to avoid damage to or loss of the physical device or data held on it.

9.10. Where there is an approved Information Sharing Agreement or Processing Agreement in place that allows a third party access to Council information, the third party is required to follow this Policy if they use removable media for the purpose of holding or transferring information. It is the responsibility of the service who share the data to ensure this Policy is followed.

9.11. Council issued removable media must not be connected to non-Council owned equipment.

9.12. 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.

9.13. 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).

9.14. Any incident where protected information is lost, damaged (physical damage to the removable media or deletion of the data upon it), leaked or put at risk must be reported as a potential data breach incident. It is the responsibility of all employees to immediately report any actual or suspected breaches in information security by informing their line manager and the Information Governance Team (information.governance@tameside.gov.uk). Failure to report any actual or suspected breach could result in an incident having more serious consequences than would otherwise have been the case and could result referral to and sanction by the Information Commissioner's Office (ICO).

9.15. All removable media devices (see definitions) should be returned to IT Services to securely delete/destroy the data and to dispose of or reallocate the removable media. This is essential to minimise the risk of the accidental disclosure of sensitive information.

9.16. For further details please refer to the IT Security Policy.

10. ACCESS CONTROL

10.1. System Access

10.1.1. Each user will be allocated access rights and permissions to computer systems and data that:

- Are appropriate for the tasks they are expected to perform;
- Have a unique login that is not shared with or disclosed to any other user;
- Have an associated unique password that complies with the Council's password guidance.

10.1.2. Where appropriate, multi-factor authentication (MFA) and/or single sign-on will be required to access Council systems.

10.1.3. System owners must review user access rights at regular intervals to ensure that the appropriate rights are only allocated to present employees of the service area and/or only to employees that require access to that system to perform their duties. System administration

accounts must only be provided to users that are required to perform system administration tasks.

10.2. Network Access Control

10.2.1. Employees are not permitted to plug in any unauthorised devices into their computer and/or the wider network. Only equipment corporately issued and/or approved by IT services is permitted; unless written permission is obtained from a SUM of Digital Tameside or the AD of Digital Tameside.

10.3. Operating System Access Control

10.3.1. Access to operating systems is controlled by a secure login process. The access control defined within this policy must be applied. The login procedure must also be protected by:

- limiting the number of unsuccessful attempts and locking the account if exceeded
- the password characters being hidden by symbols.

10.3.2. All access to operating systems is via a unique login ID that will be audited and can be traced back to each individual user. The login ID must not give any indication of the level of access that it provides to the system (e.g. administration rights).

10.3.3. System administrators must have individual administrator accounts that will be logged and audited. The administrator account must not be used by individuals for normal day to day activities.

10.4. Application and Information Access

10.4.1. Access within software applications must be restricted using the security features built into the individual product. The manager of the software application is responsible for granting access to the information within the system. The access must be:

- separated into clearly defined roles
- the appropriate level of access required for the role of the user
- unable to be overridden (with the admin settings removed or hidden from the user)
- free from alteration by rights inherited from the operating system that could allow unauthorised higher levels of access
- logged and auditable

10.5. Supplier's Remote Access to the Council Network

10.5.1. Partner agencies or Third party suppliers must not be given access to, or provided access instructions for the Council's network or any of its systems without permission from IT within a business case. Any proposed new access to the network or any system operated by the Council must be reviewed under the DPIA process, with input from Risk Management and Audit Services and the Information Governance Team. Any changes to a supplier's connections must be immediately sent to the IT Service Desk so that access can be updated or ceased. All permissions and access methods must be controlled by IT Services with assurances from the SIRO.

10.5.2. All partner agencies or third party suppliers seeking to remotely access the Council's network must, upon receiving authorisation from IT, use the remote access portal.

10.5.3. Partners or Third party suppliers must contact IT before connecting to the Council network and a log of activity must be maintained. Remote access software must be disabled when not in use.

11. COMPLIANCE

11.1. This Policy takes into consideration all applicable statutory, regulatory and contractual security requirements.

11.2. All breaches of this policy and all other personal data breach incidents, irrespective of scale, must be reported to information.governance@tameside.gov.uk within the first 24 hours of knowledge to allow for mitigations to be put in place, lessons to be learned and to improve data handling procedures and the breach response process.

11.3. Where a data breach is established to have occurred and there is a high risk of adversely affecting individuals' rights and freedoms, we are required to report to the Information Commissioners Office within 72 hours of first knowledge of the breach, without exception. Failure to report an incident to the Information Governance Team may result in disciplinary action being taken.

11.4. For further information regarding, refer to the Personal Data Breach Reporting Procedure.

11.5. It is the responsibility of all employees to ensure that they have read and comply with the conditions laid out in this protocol.

11.6. Non-compliance with this protocol could have a significant effect on the efficient operation of the Council and may result in financial loss and an inability to provide necessary services to our customers.

11.7. If any user is found to have breached this protocol, they may be subject to the Council's Disciplinary Procedure. If a criminal offence is considered to have been committed further action may be taken to assist in the prosecution of the offender(s).

11.8. If you do not understand the implications of this protocol or how it may apply to you, please contact the information Governance Team (information.governance@tameside.gov.uk) or the Council's Information Security Officer (cybersecurity@tameside.gov.uk).

12. HARASSMENT AND ABUSE

12.1. 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 Grievance Procedure (Appendix A - Bullying and Harassment). 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.

12.2. Employees should be aware that the Council Systems including the internal and external email system is monitored 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.

13. DISCIPLINARY IMPLICATIONS

13.1. Breaches of this policy may result in disciplinary action up to and including dismissal. They may also result in you being personally prosecuted under the Computer Misuse Act 1990,

Data Protection Act 2018/UK GDPR or other applicable legislation and may also lead to prosecution of the Council, fines and/or civil claims for damages.

13.2. Misuse of Council owned IT equipment or software may also be a breach of the statutory Code of Conduct for Councillors, or other regulatory codes of conduct for professional occupations (Social workers, Solicitors etc.). Breaches of this policy may be reported to the relevant regulatory body.

14. DEFINITIONS

14.1. The following terms are referenced throughout this document and are defined as follows:

Term	Definition
Employee(s)	Includes all employees, Members of the Council, Committees, temporary staff, volunteers, contractual third parties, partners or agents of the Council who have access to any information systems or information for council purposes.
Equipment	Includes, but is not restricted to, the following: • Servers • Laptop and desktop PCs • Mobile phones / Smartphones • Tablets • Printers / scanners • Personal Digital Assistants (PDA's) • Text pagers • Wireless technologies • Digital Cameras and other photographic or video recording equipment (CCTV cameras, body cameras, dash cams, drones etc.) • MP3 Players
Personal Data	Is any personal data as defined by UK GDPR and the Data Protection Act 2018. It is defined in the Data Protection Act 2018 at **s.3 (2)** as "any information relating to an identified or identifiable living individual." Broadly this means any information (relating to a living individual) who can be identified or identifiable, directly from the information in question, or indirectly identified from that information in combination with other information that is in the possession of the Council. The UK GDPR provides a non-exhaustive list of identifiers, including: • Name; • Identification number; • Location data; and • Online identifier (e.g. IP addresses).

APPENDIX 2

Term	Definition
	Personal data also applies to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of a living person. The Council is legally responsible for the storage, protection and use of personal data / information held by it as governed by UK GDPR and the Data Protection Act 2018.
Protected Information	Is any information which is: • Personal / Special Category Data; or • Confidential to the Council and which could have adverse consequences for the Council if it was released in an uncontrolled way.
Removable Media	Storage devices including, but not limited to, USB memory sticks, CDs, DVDs, SIM cards, memory cards, magnetic tapes, external/portable hard drives, solid state drives, digital cameras and / or other video recording equipment
Special Category Data	This data is covered by Articles 6 and 9 of the General Data Protection Regulations (UK GDPR). As it is more sensitive it needs more protection and consists of: • Racial or ethnic origin • political opinions / beliefs • religious or philosophical beliefs • trade union membership • genetic data • biometric data (where used for ID purposes) • health; • sex life; or • sexual orientation. Criminal Offence Data is not Special Category Data, but there are similar rules and safeguards for processing this type of data.