



IT Security Policy

DRAFT

Date: December 2023

Version: V1.2

Document Version Control

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

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 It supersedes any previous versions of this document, which are now withdrawn.

DRAFT

Contents

Document Version Control	2
1. INTRODUCTION.....	4
2. EQUIPMENT (EMPLOYEE RESPONSIBILITIES).....	4
3. EQUIPMENT (RETURN AND DISPOSAL).....	5
3.3. Staff Leavers	5
3.4. Internal movers.....	5
3.5. Moving equipment	6
4. TRAINING	6
5. MANAGEMENT OF DATA, INFORMATION AND SOFTWARE.....	6
6. AUTHORISED BUSINESS USE	6
7. UNAUTHORISED USE	7
8. SECURITY	7
8.1. Access to Council systems.....	7
8.2. Passwords	7
9. PERSONAL USE	8
10. THE COUNCIL'S RIGHTS AND OBLIGATIONS	8
11. CYBER SECURITY	9
11.3. Phishing	9
11.4. Malicious Software ('Malware')	9
12. USE OF IT AT HOME OR OUT OF THE OFFICE	10
13. BACK UPS	10
14. CONTRAVENTIONS OF THE POLICY.....	10
15. DISCIPLINARY IMPLICATIONS	10
16. PERSONAL DATA BREACH INCIDENTS	10
17. DEFINITIONS.....	11

APPENDIX 1

1. INTRODUCTION

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

- Preserve the confidentiality, integrity and availability of its data/information;
- Ensure an approach to security in which all employees fully understand their own responsibilities;
- Ensure that all employees are aware of and fully comply with the legislation as described in this and other policies;
- Minimise legal and other risks associated with the use of technology;
- Detail how to protect the data/information assets under the Council's control;
- Get the best return possible for the investment it has made in technology;
- Ensure effective running of the Council's business;
- Use technology to maximise flexibility around new working practices;
- Minimise the risk of disruption caused by malware and inappropriate use of IT; and
- Provide clear information to employees and increase the IT skills of our employees and residents.

1.2. This policy sets out the Council's policy on using its IT equipment and its internal and external infrastructure ('systems').

1.3. This policy applies to all Council employees who use the Council's equipment and systems.

2. EQUIPMENT (EMPLOYEE RESPONSIBILITIES)

2.1. All employees have responsibility for the equipment they use and the data/information accessed through and stored on that equipment. Everyone using Council equipment must adhere to the below points regarding Council Equipment and Data.

2.2. If equipment malfunctions you should contact the IT Service Desk for advice and assistance. Employees must not attempt to repair or maintain their IT equipment, except for day-to-day needs such as replacement ink cartridges in printers etc. All employees are expected to look after any Council equipment as if it was their own personal equipment, to ensure it is kept in good working order.

2.3. 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. Smartphones will be provided with a protective case which must be used at all times. Any deliberate damage could result in the employee being personally liable for the cost of repair or replacement of the damaged equipment.

2.4. Damaged equipment must not be disposed of by individuals and should be returned promptly to IT Services. This is to ensure the safe removal of any licences or data from the device.

2.5. Employees are the last line of defence against cyber-attack. Every employee has a responsibility to use their equipment safely and responsibly to avoid exposing the Council's systems to cyber-attack.

2.6. Every employee has a duty to ensure that any and all equipment provided to them is kept secure from loss, theft or attack. This particularly applies to portable equipment such as laptop computers, tablets and mobile phones. The Council carries insurance for incidents

APPENDIX 1

beyond an employee's control within the UK, but if equipment is lost as a result of an employee's negligent or deliberate act then disciplinary action may be taken and the Council may take action to recover the cost from the employee concerned. Any queries about this should be referred to the Insurance Team (insurance@tameside.gov.uk).

- 2.7. Where the Council provides a laptop to an employee, 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 logging the device off (selecting "shut down" and waiting until the process is complete before closing the device).
- 2.8. All Council equipment must be purchased through IT Services using the Council's approved procurement facility. For the avoidance of doubt, it is not permitted for any manager or employee to purchase IT equipment themselves and reclaim the cost through the expense system. Any equipment not procured through IT Services poses a security risk to the integrity of the Council's systems and/or the data/information stored or processed on the unsanctioned piece of equipment.

3. EQUIPMENT (RETURN AND DISPOSAL)

- 3.1. All equipment must be disposed of through IT Services to ensure that legislation is complied with both in respect of the environment and security of information. Moving IT 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 legislation.
- 3.2. When IT Services receive equipment back, they will determine whether the equipment can be repurposed for further use within the Council, or is to be disposed of securely. Where equipment cannot be reused, it is disposed of via a third party contractor, who will comply with relevant industry standards to safely dispose of the equipment, meeting all regulatory and legislative requirements, including effective destruction of any data held on the equipment. Where the equipment can be repurposed, it will be securely wiped to ensure all data is removed before reallocation to another user.

3.3. Staff Leavers

- 3.3.1. 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. This will ensure the correct system accesses are removed and the return of all equipment is arranged on the leaver's final working day or as soon after as is possible. Managers are accountable for making sure this is strictly complied with. Failure to return the equipment promptly to IT will result in a data breach being recorded against the manager and also could lead to the matter being reported to the police as stolen property. We reserve the right to seek recovery of replacement costs of equipment and associated costs from employee's. Please note that the service area is initially charged replacement cost for any non- returned equipment.

3.4. Internal movers

- 3.4.1. 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.
- 3.4.2. The manager of the new team will log a "new starter" ticket on the IT Service Desk.
- 3.4.3. The full process for staff movers can be found in the [IT Acceptable Use Policy](#)

3.5. Moving equipment

- 3.5.1. Where equipment, such as desktop PCs, printers/scanners, servers etc. need to be relocated, IT Services must be contacted to carry this out. Equipment must only be moved by IT Services.

4. TRAINING

- 4.1. All employees are expected to undertake IT training, and mandatory Information Governance training as directed where they handle any data as part of their day to day role. The Information Governance training is required to be completed on an annual basis.
- 4.2. The IT Induction training is mandatory and will be provided to all new starters as they collect their IT equipment. IT equipment including passwords will not be issued until the induction has taken place. By exception (for example where a new starter does not live locally), equipment can be issued but passwords will be withheld until the induction has taken place either in person or remotely.

5. MANAGEMENT OF DATA, INFORMATION AND SOFTWARE

- 5.1. Employees are expected to manage data in compliance with the legislation relating to data protection and freedom of information. The Data Protection/Information Governance Framework and supporting policies, protocols, procedures and guidance documents <https://intranet2.tameside.gov.uk/infogov> 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, in line with the corporate [Retention and Disposal Guidance/Schedule](#)
 - Keep data secure
 - Keep data confidential.
- 5.2. The Council has legal duties under the Data Protection Act 2018 and Computer Misuse Act 1990 to protect the information that it holds. No personal information should be disclosed unless you are sure that you are permitted to do so and the appropriate data sharing or processing agreements are in place. If any employees have any further queries they should seek advice from the Information Governance Team (information.governance@tameside.gov.uk).

6. AUTHORISED BUSINESS USE

- 6.1. You may use the Council's 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 10 of this policy.
- 6.2. Each day as you log onto your device you will be presented with a screen confirming you agree to comply with the Council's policies including but not limited to this Policy, the Acceptable Usage Policy and the Information Governance Policies.
- 6.3. In order to ensure accountability in the use of the Systems, you must only use the equipment you have been personally allocated by IT Services.

APPENDIX 1

- 6.4. Employees may only use software officially purchased, issued and approved by IT Services as the Council is under an obligation to ensure that all software is properly licensed and approved and that the individual and business intellectual property rights in respect of that software are protected at all times. Users breaching this requirement may be subject to disciplinary action.

7. UNAUTHORISED USE

- 7.1. There are controls in place to ensure that employees cannot misuse the Council's systems or software. Employees must not use any software, including cloud service, which has not been officially purchased, issued or approved by IT Services and been through the DPIA process. Employees must not copy or attempt to copy any of the software on the Council's Systems. Software will be audited on a regular basis.
- 7.2. You must not connect any equipment to the Council's Systems unless it belongs to the Council and you have the express permission of IT Services.
- 7.3. You must not misuse the Council's Systems by accessing information which you are not authorised to view or use in performance of your duties. Access to any data for personal use is strictly prohibited and will result in disciplinary action. You must not attempt to break ('hack') into any computer system, for example by using someone else's password.

8. SECURITY

8.1. Access to Council systems


- 8.1.1. Maintaining the security of the Council's network and IT systems is vitally important. Formal user access control procedures must be documented, implemented and kept up to date for each application and information system to ensure only authorised user access and to prevent unauthorised access.
- 8.1.2. Each user must 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 (see section 9.2).
- 8.1.3. Where appropriate multi-factor authentication (MFA) will be added to Council systems as an additional layer of security.
- 8.1.4. User access rights must be reviewed at regular intervals to ensure that the privilege of least access is being implemented – that is that 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.
- 8.1.5. For further guidance, please refer to the [IT Acceptable Use Policy](#).

8.2. Passwords

- 8.2.1. You will be issued with unique passwords for accessing the Council's Systems. You must keep your password confidential and you should not disclose your password to anyone else.

APPENDIX 1

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.

- 8.2.2. 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 guessed by others (e.g. the names of partner, children or pets). All employees must adhere to the [IT Corporate Password Policy](#).
- 8.2.3. When you have logged into any computer you should ensure that it is left securely so that no unauthorised person can access it. Whenever you leave your computer (whether working in a Council premises, at home or a third party premises), you must lock it by pressing 'Ctrl + Alt + Delete' and then confirming that you wish to lock your workstation, or by pressing 'Windows key () + L'.
- 8.2.4. If you have been issued with a portable device (mobile telephone, tablet etc.) this should be password/pin code protected and locked at all times when not in active use. You must not store the pin code with the device. When you leave your work area you should take the portable device(s) with you, or store away safely.
- 8.2.5. Personal or confidential data/information 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 IT Services. Where such data/information is permitted to be 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 IT Acceptable Use Policy.

9. PERSONAL USE

- 9.1. 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.
- 9.2. 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.
- 9.3. 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.
- 9.4. 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.

10. THE COUNCIL'S RIGHTS AND OBLIGATIONS

- 10.1. The Council reserves the right to monitor all communications and information created, or transmitted on its 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 Data Protection legislation and the Council's Data Protection/Information Governance Framework.

11. CYBER SECURITY

- 11.1. The Council has comprehensive security and antivirus protection systems in place, which protect devices that connect to the council's network and keep thousands of spam emails and viruses from reaching Council mailboxes every month.
- 11.2. Only equipment or systems which have antivirus installed can be connected to the Council's network, unless written permission is obtained from a SUM of Digital Tameside or the AD of Digital Tameside.

11.3. Phishing

- 11.3.1. Phishing is a type of social engineering attack in which cyber criminals trick victims into handing over sensitive information or installing malware. E-mail is currently the most vulnerable method for phishing, malware and identity theft. If you receive an email from an unknown source, or containing content which looks suspicious you can report this directly from your Email client by right clicking on the email in the list and selecting 'Report as Malicious'
- 11.3.2. If you think you have clicked on a phishing email, or opened a suspicious attachment switch off your computer immediately and report this to IT services.

11.4. Malicious Software ('Malware')

- 11.4.1. Malware' is a collective term used for malicious software - viruses, worms, spyware, rootkits, botnets, ransomware etc. A virus is a piece of self-replicating computer program code that is designed to destroy or damage digital information, or to steal user and/or business data.
- 11.4.2. There are many potential sources of malware, including websites, social media, removable media such as USB memory sticks and CDs, email, and software or documents downloaded off the internet.
- 11.4.3. 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.
- 11.4.4. A malware infection can be incredibly costly for the Council and can often be time-consuming for all involved. This may be through the loss of data or access to IT systems, staff time to recover the systems, and/or the delay or loss of council data. Additionally, malicious software can spread from an infected system and can lead to severe disruption to IT services and possible reputational damage or even fines from the Information Commissioner's Office (ICO). Malicious software is a constantly evolving threat and the Council therefore applies controls to protect our systems and information from all forms of malware.
- 11.4.5. Specifically, users are prohibited from:
 - Uninstalling and/or attempting to reconfigure anti-malware, updates, logging or other protective services on the Council's systems;
 - Negligently, intentionally or recklessly, introducing any form of malware;
 - Sharing login credentials with another user;

APPENDIX 1

- Using personal email accounts instead of a Council email account to conduct Council business, and/or forwarding emails from a Council email account to a personal account;
- Introducing data-interception, password detecting or similar software or devices to the Council's network;
- Seeking to gain unauthorised access to restricted areas of the Council's network;
- Accessing or attempt to access data where the user knows or ought to know that they should have not have access.
- Attaching any device or removable media (e.g. CD, memory stick) to Council equipment without submitting it to IT Services for virus checking.

11.4.6. Failure to adhere to the above could result in disciplinary action and if necessary, referral to the Police.

12. USE OF IT AT HOME OR OUT OF THE OFFICE

12.1. The provisions of this Policy apply equally when working on Council data or equipment whether working in a corporate office location or outside of Council premises.

12.2. The use of personally owned equipment to access or store council data is prohibited.

13. BACK UPS

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

13.2. All employees must be aware that IT 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.

14. CONTRAVENTIONS OF THE POLICY

14.1. Employees should be aware that the Council Systems including the internal and external email 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.

15. DISCIPLINARY IMPLICATIONS

15.1. Breaches of this policy may result in disciplinary action up to and including dismissal and may also result in referral to any professional regulatory bodies. Breaches may also result in employees 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.

16. PERSONAL DATA BREACH INCIDENTS

16.1. All breaches of this policy and all other personal data breach incidents, irrespective of scale, must be reported to the Information Governance Team (information.governance@tameside.gov.uk) within the first 24 hours of knowledge to allow

APPENDIX 1

for mitigations to be put in place, lessons to be learned and to improve data handling procedures and the breach response process.

16.2. 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.

16.3. For further information regarding, refer to the [Personal Data Breach Reporting Procedure](#).

17. DEFINITIONS

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

Term	Definition
Cloud services / infrastructure	Cloud services include infrastructure, platforms or software hosted by third-party providers and made available through the internet.
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 <ul style="list-style-type: none"> • 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 • Storage devices including, but not limited to, sim cards, flash memory cards, CDs, DVDs, magnetic tapes, portable hard drives and USB memory sticks.
Hybrid 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 their home, Council Workspaces, customer sites, Touch Down Points etc.)
Infrastructure	An encompassing term to cover all components required to enable IT operations. Includes but is not restricted to, the following <ul style="list-style-type: none"> • Hardware • Software • network resources • servers • computers

APPENDIX 1

Term	Definition
	<ul style="list-style-type: none"> • switches • Access Points
Legislation	<p>Includes but is not restricted to:</p> <ul style="list-style-type: none"> • The Computer Misuse Act (1990); • The Copyright, Designs and Patents Act (1988); • The Data Protection Act 2018; • The Freedom of Information Act 2000; • The General Data Protection Regulations (UK GDPR); • The Regulation of Investigatory Powers Act 2000.
Personal (Wi-Fi) Hotspot	<p>A wireless internet access point provided by a smartphone.</p>
Personal Data	<p>Is any personal data as defined by UK GDPR and the Data Protection Act 2018.</p> <p>It is defined in the Data Protection Act 2018 at s.3 (2) as “any information relating to an identified or identifiable living individual.”</p> <p>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.</p> <p>The UK GDPR provides a non-exhaustive list of identifiers, including:</p> <ul style="list-style-type: none"> • Name; • Identification number; • Location data; and • Online identifier (e.g. IP addresses). <p>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.</p> <p>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.</p>
Protected Information	<p>Is any information which is:</p> <ul style="list-style-type: none"> • 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.
Special Category Data	<p>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:</p> <ul style="list-style-type: none"> • Racial or ethnic origin

APPENDIX 1

Term	Definition
	<ul style="list-style-type: none">• 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. <p>Criminal Offence Data is not Special Category Data, but there are similar rules and safeguards for processing this type of data.</p>
VPN (Virtual Private Network)	Refers to a secure network connection that uses the internet to transmit data. It allows employees to access the Council network out of the office from a Council issued laptop.