# Computer Usage Policy

*Document control:*

| | |
|---|---|
| *Version:* | 2022 - 01 |
| *Author:* | Julie May |
| *Status:* | Published |
| *Publication date:* | 22nd May 2018 |
| *Next review:* | 1st April 2023 |

## Contents

## 1. Purpose

1.1 The purpose and objective of this Policy is to outline to computer users their responsibilities whilst using the council's computers, mobile phones, network infrastructure and associated software and data in a safe and secure manner. This applies when using corporate or personal ICT hardware connected to the corporate network or processing corporate data from any location.

1.2 The policy has been developed to support the council's compliance requirements:

- General Data Protection Regulations
- Data Protection Act
- Freedom of Information Act
- Environmental Information Regulation
- Public Services Network Code of Connection
- Payment Card Industry Data Security Standards

## 2. Scope

2.1 The policy applies to all employees, Councillors, partners, contracted third parties and other agents of Maidstone Borough Council, Swale Borough Council and Tunbridge Wells Borough Council (hereafter referred to as "the council") who have access to information systems or information used for council business – (hereafter referred to as "users").

2.2 An additional policy document ("Third party Computer Usage Policy") is distributed to third parties and in all cases where the user is not employed by the council. Both documents must be signed before network access is provided.

2.3 It is the responsibility of managers to exercise appropriate controls to minimise the risk of misuse and where misuse is found to report it to HR, a manager, or in the case of a security breach – through the process described in "Appendix C – Reporting a digital security incident".

2.4 For the purposes of this policy, "the council's network" is that which is managed by Mid Kent ICT Services on behalf of the council.

## 3. Policy management

3.1 This policy is communicated to users electronically and all users must confirm they have read and understood the policy before being provided with Mid Kent ICT facilities and services.

3.2 It will be reviewed annually by the Mid Kent ICT Management Team and proposed changes escalated through the policy management process of the council.

3.3 Changes will be distributed electronically, clearly stating where the policy has changed.

3.4 Network access will be blocked until the user has accepted the changes to the policy, although a grace-period of three logins will be provided.

3.5 The policy will be monitored and reviewed regularly by MidKent ICT and matters of non-compliance escalated where appropriate to the Management Teams of the relevant authority.

3.6 Minor changes and updates to the policy will be made on an ad-hoc basis by the Mid Kent ICT Management Team and circulated as necessary. Members of staff will not need to confirm understanding in these instances.

3.7 It is the user's responsibility to seek clarification from their line manager for any aspect of the policy which they do not fully understand.

## 4. Key points

4.1.1 The policy ***must*** be read in full, but for future quick reference the key points are outlined below:

- Passwords must **never** be shared or written down.
- Never leave your laptop, tablet or mobile phone unattended or unlocked when not in use.
- Files containing sensitive data must not be saved on local devices such as the *desktop* or hard drive of a laptop.
- Only use email for **work purposes** and consider what is appropriate to send in an email as it can be retrieved by your employer in certain circumstances.
- Do not forward council emails to or respond to them from your personal email account.
- Security incidents **must** be reported immediately to the Senior Risk Information Owner (SIRO), Mid Kent ICT, your manager and where appropriate the Data Protection officer.
- "BCC" must be used instead of "CC" where any recipients outside the Council are not known to each other and there is not valid reason to share email addresses. See section - 6 email policy – for more information.
- Personal web browsing is permitted in your own time, but subject to filtering and logging for inspection and analysis at a later date.
- Your Internet browsing history can be retrieved and a strict policy is in force that blocks access to websites that our filtering system is unaware of. You will need to request access to them through the Mid Kent ICT Service Desk.
- Removable media such as memory sticks **must** be encrypted. Mid Kent ICT Service Desk can assist you. If there are specific technical reasons that encryption cannot be used then a business case and risk assessment must be submitted to Mid Kent ICT Services so that an informed judgement can be made.
- A breach of this policy could result in disciplinary action under the Council's procedures.
- Non-employee users of the facilities who breach the policy may have their access to the facilities withdrawn and, depending on the nature of the breach, may be liable to legal proceedings.

## 5. Password policy

5.1 Access to the council's network and ICT resources is through a combination of user name and password which must meet the following complexity requirements:

- The minimum length of any password must be seven characters;
- They must include a combination of letters, numbers, and/or symbols;
- It cannot include a word from your name as recorded in the network user directory.

5.1.2 Passwords will expire after 90 days at which point you will be required to choose a new password before network access can continue.

5.1.3 Password history for network access includes your last 20 passwords, which cannot be re-used.

- Historic passwords are stored in an encrypted format in the network account directory – the same location as your current password.
- Do not simply change the number at the end of a password.

5.1.4 Passwords must be kept confidential and must not be shared with other users.

- It is recognised that there will be instances where credentials need to be shared, such as social media accounts operated by multiple members of staff. In these circumstances a business case and risk assessment must be presented to the council's DPO for approval. When a member of staff legitimately sharing a password leaves the employment of the council or changes role then the password must immediately be changed.

5.1.5 Paper or unsecured electronic copies of personal passwords must not be kept. Advice on secure electronic storage of passwords can be obtain from the ICT Service Desk.

5.1.6 You must avoid easily guessable passwords such as names.

5.1.7 When changing your password the system will automatically reject any passwords that do not meet the complexity, reuse and age policy described above.

5.1.8 A password can be attached to biometric data on equipment and software that supports it.

## 6. Email policy

6.1 Email facilities are provided for business purposes in order to enhance the working environment.

6.2 External e-mails have the same status as a written, formal letter from the council and will be treated as such by recipients. A signature block must be attached to all emails following the council's own guidelines.

6.3 E-mail communication using the council's network or computing resources is the property of the council and is subject of Freedom of Information requests and Data Protection Subject Access requests.

6.4 You must not reply or click on a link within a "spam" or unsolicited email as this presents a security risk to the Council.

6.5 The use of the council's resources for personal gain or for any purpose that is illegal, contrary to the council's policies for general conduct or which is known to be contrary to the council's interest is prohibited and may lead to disciplinary action.

6.6 Staff should review "Appendix A - Examples of inappropriate use of communications facilities" for a list of what should and should not be used in electronic communications.

6.7 Access to e-mail must be via the council's chosen e-mail applications (see Appendix B – List of supported mail applications)

6.8 The council automatically records email activity and content in a searchable archive. This may be used as evidence in any suspected cases of misuse or misconduct by the user. The Council's monitoring procedure is described in Appendix D – Monitoring Computer Use.

6.9 The council's automated email content scanning system exists as a barrier to content that is or it suspects may be a danger to our service provision. It blocks the delivery of emails that flag up under certain conditions such as file size, file type and message body content (e.g. bad language, credit card numbers etc.)

6.10 The file attachment size limit and other blocking rules are available on the ICT Customer Portal in the FAQ section searching by searching for "quarantined".

6.11 In the event that an inbound or outbound email is quarantined by the content scanning system, a limited number of ICT staff will have access to the message body and attachment. They will make an informed judgement as to whether it should be released for delivery.

6.12 Emails are the property of the Council and are subject to disclosure through Freedom of Information requests and Subject Access requests. The Council alone has the right to determine whether the content of an email should be disclosed, and under what conditions.

6.13 It is understood that staff may from time to time receive information not related to their job on their work emails. The council asks that usage is limited by the staff member. Staff must not use their work email accounts to sign up to any websites that are not work related such as shopping sites for example.

6.14 The council also reserves the right to access your work email account in mitigating circumstances.

## 7. Use of the Internet for web access

7.1 Attempts to access websites that are offensive or inappropriate are automatically blocked and recorded with a date, time and user name.

7.2 The Council has the right to determine what is offensive or inappropriate when using Council resources, but as a minimum will include anything prohibited by law.

7.3 The impersonation of any individual or organisation is not permitted when using any of the council's ICT systems, such as web sites (including social media) and email.

7.4 Websites that are blocked by category and need to be accessed to conduct council business can be made available by contacting the Mid Kent ICT Service Desk. Authorisation from your line manager is required before access is granted.

7.5 Websites that are blocked and do not have a category within the filtering system can be unblocked without a manager's approval at the discretion of Mid Kent ICT Services.

7.6 Accidental viewing of materials which infringes those mentioned above must be reported according to the Digital security incident reporting procedure – "Appendix C – Reporting a digital security incident".

7.7 Monitoring of Internet use

7.7.1 Use of the Internet is recorded and may be monitored if the Council suspects misuse or misconduct by a user. Access to the Internet may also be withdrawn. The Council's procedure for monitoring computer use is described in Appendix D – Monitoring Computer Use.

7.7.2 It is possible to identify internet sites visited by individual users. The council reserves the right to inspect any files at any time during investigations where there is suspected misuse and to withdraw access to the Internet.

7.8 Personal use of the Internet

7.8.1 The council allows web browsing primarily for business use. Occasional and reasonable personal use is permitted in your own time.

7.8.2 Personal use is defined as any activity that is not work-related or necessary in the performance of duties connected to your employment. The personal use of the Internet for any purpose must be in the employee's own time and at no additional expense to the council, and must not interfere with the employee's ability to conduct their normal duties.

7.8.3 Employees must exercise the same degree of care and awareness of security issues with personal use of the Internet at work as they would with work-related use.

7.8.4 No liability can be accepted by the Council for any loss that an individual may suffer as a result of personal use of council owned ICT equipment.

7.8.5 Personal email addresses must be used for subscription to email mailing lists and list servers for personal purposes. Corporate email address must not be used as they present a security risk in the event that the provider experiences a data leak.

7.8.6 In the event of loss or damage to software and / or hardware arising out of personal use recompense may be sought by the council.

7.9 Software downloads and uploads

7.9.1 You must not download or attempt to install software (either corporate or personal) without the express permission of Mid Kent ICT Services. This includes software for trial purposes.

7.10 Purchasing of goods or services

7.10.1 The purchasing of goods or services via the Internet is subject to the council's financial rules or procedures.

## 8. Digital security incidents

8.1 A digital security incident occurs when data or information is transferred or is at risk of being transferred to somebody who is not entitled to receive it.

8.2 The responsibility for reporting digital security incidents lies with the user and must be carried out immediately by phone and followed up in writing to the SIRO, the Mid Kent ICT Service Desk and to the Data Protection Officer (DPO) where personal data is or may be involved.

8.3 The SIRO may be required to escalate the incident to the Information Commissioner's Office (ICO) and notify any data subject(s) affected.

8.4 The responsibility for managing digital security incidents lies with the SIRO where personal data is involved, or with ICT Network Manager if personal data is not involved.

8.5 A *digital security incident* includes:

- The loss or theft of data or information;
- The holding to ransom of data or information;
- The introduction of a virus / malware onto a device that is or can be connected to the council's ICT systems and infrastructure.
- The loss or theft of equipment which may provide access to data or information;
- The transfer of data or information to those who are not entitled to receive that information;
- Attempts (either failed or successful) to gain unauthorised access to data or information storage or a computer system ;
- Changes to information or data or system hardware, firmware, or software characteristics without the council's knowledge, instruction, or consent ;
- Unwanted disruption or denial of service to a system;
- The unauthorised use of a system for the processing or storage of data by any person.

8.6 When to report

8.6.1 All events that result in the actual or potential loss of data, breaches of confidentiality, unauthorised access or changes to systems must be reported as soon as they happen.

8.6.2 The process for reporting a digital security incident is described in "Appendix C – Reporting a digital security incident"

8.6.3 Internal Audit will be informed by the Network Manager as the controls in place may need to be investigated.

## 9. Portable devices (laptops, tablets and mobile phones)

9.1 Use of portable devices

9.1.1 This policy is designed to safeguard both the council and users of mobile phones, laptops and tablets supplied by the council, or their own personal devices, which have council-owned software installed or access to council-owned data. It aims to ensure that these devices are used effectively, for their intended purposes and without infringing legal requirements or creating unnecessary business risk. Its aims are to:

- ensure that all users understand how portable devices supplied by the council should and should not be used;
- protect both the council and individuals from the possibility of legal action.
- protect the council's information technology systems against damage from mobile phones which have email and internet facilities.

9.2 General principles

9.2.1 You must not download sensitive data to your device and store it on the *desktop*, hard drive or any removable media such as a USB drive.

9.2.2 You must not use the device in any way which is inconsistent with carrying out your job or might conflict with the council's interests.

9.2.3 You must not use the device to access, use or distribute any material, or to participate in any activity, which is, or might reasonably be regarded as, distasteful, offensive or indecent or harmful to other users. Refer to Appendix A - Examples of inappropriate use of communications facilities – for more information.

9.2.4 You must not use the device to:

- download applications which are not work-related without the approval of Mid Kent ICT Services.
- carry out any business activity either for yourself or on behalf of someone else;
- upload, download or otherwise transmit commercial software or other material, in violation of its copyright.

9.2.5 If you identify any abuse or misuse of a device you must report it to your manager and Mid Kent ICT Services immediately.

9.3 Personal use of corporate portable devices

9.3.1 The council provides corporate portable devices to help you to carry out your job and the provision of the device is subject to the separate Mobile Device policy.

9.4 Use of personal mobile devices

9.4.1 Personal mobile phones can be used to access mail, calendar and contact services as well as Unified Communications.

9.4.2 A request must be submitted to Mid Kent ICT Service Desk and the user will be asked to sign a document agreeing to software being loaded on the device that enforces secure access controls such as PIN codes and the ability to remote wipe the council's data or, if requested by the owner, then entire device, in the event a device is reported lost or stolen.

9.4.3 In the event that a personal device is lost or stolen it must be reported to the Mid Kent ICT Service Desk and the DPO immediately.

9.5 Portable device security

9.5.1 Care must be taken to ensure that all devices are kept securely.

- They must not be left unattended in vehicles or areas of the workplace that are accessible to the public.
- Non-Windows devices such as mobile phones have security lock codes enforced.

9.5.2 Any attempt to circumvent any security settings or software implemented by the Council is deemed a breach of this policy.

9.5.3 Mobile phone users must adhere to the legal requirements *and* the council's policy on the use of mobile phones while driving.

9.5.4 Once a device has been replaced or upgraded due to age or where a device becomes surplus they must be labelled for recycling and returned to the Mid Kent ICT Service Desk.

## 10. Unified Communications usage

10.1 A Unified Communications (UC) system delivers voice calls, video conferencing, Instant Messaging (IM), chat rooms, presence and location information for users of the Mid Kent ICT network.

10.2 The council reserves the right to monitor such data via its system reporting tools.

10.3 The council's Instant Messaging facility is provided via MS Teams and is intended for business purposes in order to benefit users and to enhance the working environment. Chat conversations can be carried out internally across the three Mid Kent partner councils and where enabled, with federated organisations outside of the partnership. A full list of those organisations that are federated is available from Mid Kent ICT.

10.4 Use of Chat on the Council's network is not routinely monitored but chat history is saved on the Mid Kent ICT network. Staff should be aware that confidential information should not be discussed on chat.

10.5 Chat is appropriate for informal business use only.

10.6 Inappropriate use of Chat is prohibited. Offensive or inappropriate language, views or pictures may result in disciplinary action. See "Appendix A - Examples of inappropriate use of communications facilities".

## 11. Applications and systems

11.1 Line of business applications (henceforth referred to as “applications”) are used to carry out the business of the Council in one or more service areas. Examples include Document Management systems, Customer Relationship Management Systems and Website Content Management systems.

11.2 Ownership of each application rests with the service that primarily uses it, henceforth referred to as the “owner”.

11.3 The owner is responsible for maintaining a business relationship with the supplier and obtaining regularly updated product roadmaps that outline planned upgrades and the product lifecycle. This information must be communicated to Mid Kent ICT to inform medium and long term resource and capacity planning.

11.4 The owner is responsible for providing the necessary budget codes in order to pay invoices to the supplier.

11.5 Invoices will be approved by Mid Kent ICT before payment can be made.

11.6 The owner will delegate a named individual to liaise with Mid Kent ICT Services in all matters relating to the application.

11.7 The owner will inform Mid Kent ICT Services of any planned increase in cost as soon as the supplier notifies the Council.

11.8 Procurement of line of business applications (new and upgraded) must be approved by the Joint ICT Commissioning Group, for which the Council provides a representative.

11.9 Unless other arrangements have been made, the owner is responsible for maintaining the user database and assigning appropriate permissions and removing them when a user either leaves the employment of the Council or no longer requires access to the application to carry out their duties.

11.10 The application must conform to the password policy in section 5. Where this cannot be achieved, agreement from the Head of ICT must be obtained before the application can be procured, installed or used.

11.11 The policy applies to all applications, regardless of their location; the Mid Kent Data Centre or “cloud-based”.

## 12.Use of OneDrive

12.1 Share files with specific individuals never with everyone ot the public

12.2 Be careful sending links to shared folders because they can often be forwarded to others who you did not provide access to.

12.3 Remember once you have shared a file with someone they can download it to their device and share it with others

12.4 Remove individuals access once they no longer need ot

12.5 Be mindful of sharing files and folders that contain sensitive/confidential information if you are in any doubt contact your Data Protection Team.

## Appendix A - Examples of inappropriate use of communications facilities

The following are examples of inappropriate use of the email, instant messaging, text messaging and other communications facilities provided by the council.

- transmitting, retrieving or storing any communications of a discriminatory, harassing, obscene or pornographic nature, or for advertising such materials
- having content which may be considered by the recipient as derogatory or inflammatory in relation to race, age, disability, religion, ethnic origin, physical attributes or sexual preference
- containing material that may be classed as harassment, e.g. material of an aggressive, abusive, bullying, offensive, libellous, derogatory or anti-social nature, or may reasonably be considered in bad taste
- communicating extreme views which could be to the detriment of the council or its reputation
- responding angrily or defensively to perceived criticism or derogation
- containing any information or data that contravenes the Data Protection Act 1998
- containing anything that may bring the council, its members or officers into disrepute
- being used to participate in chain or pyramid letters or other such schemes
- being used to sign-up to non-work-related websites and services

## Appendix B – List of supported mail applications

The council's email system is Microsoft Exchange online. The ICT Service Desk can only provide support for users running Microsoft Office 365 on equipment owned and managed by the council.

Where users are operating their own equipment to read their mail in a web browser ("webmail") and on personal mobile phones and tablets, best endeavours will be made to resolve any issues, but it must be accepted that they will not be able to resolve all issues.

## Appendix C – Reporting a digital security incident

The SIRO, ICT Service Desk and where appropriate the Data Protection Officer, must be initially contacted by telephone or in person and followed up in writing. In the event that they are not contactable then every effort must be made to pass on a message through your line manager.

For SIRO and Data Protection Officer (DPO) contact details refer to Appendix E – Role descriptions and contact details.

The ICT Service Desk and DPO will require you to supply further information, the nature of which will depend upon the type of the incident. The following information must be supplied:

- Contact name and number of person reporting the incident;
- The type of data or information involved;
- Whether the loss of the data puts any person or other data at risk;
- Location of the incident;
- Inventory numbers of any equipment affected;
- Date and time the security incident occurred;
- Location of data or equipment affected;
- Type and circumstances of the incident;
- Police crime number if a device has been reported stolen.

Your line manager must also be informed to enable them to assist in any investigation. Where personal data is involved the DPO will inform the Information Commissioner's Office and will perform an investigation in accordance with the Data Protection Act Breach Reporting Procedure. The Network Manager may also investigate the issue. The outcomes of these actions are to be reported to the ICT Service Desk for inclusion in the incident details for the Network Manager's investigation.

# Appendix D – Monitoring Computer Use

## What is workplace monitoring?

Employers have the right to monitor activities in many situations at work. Examples of monitoring in the workplace include:

- recording on CCTV cameras
- opening mail or e-mail
- use of automated software to check e-mail
- checking phone logs or recording of phone calls
- checking logs of websites visited
- collecting information to check the performance of individual operators.

All of these forms of monitoring are covered by data protection law. Data protection law doesn't prevent monitoring in the workplace. However, it does set down rules about the circumstances and the way in which monitoring should be carried out.

## Who carries out the monitoring?

ICT staff may monitor logs kept by systems or applications and will report potential breaches. Monitoring is generally an automated process, with reports available upon request. However, if an email is quarantined due to content that the scanning system considers suspicious, ICT staff will be able to read the content of the quarantined message.

## What is the Council's process for requesting the monitoring of computer use?

Many applications collect usage data continuously as part of a security or auditing system and record it against a specific user name. The Council does not routinely monitor such data, but will do so upon request from a manager, HR or law enforcement agencies.

In the event that a manager needs to carry out an investigation, they will first obtain approval from HR, providing a reason for the investigation.

HR will provide a written request to the Head of ICT, Chief Operations Officer, Network Manager or Service Desk Manager detailing the name of the individual, the application logs to be queried, and the start and end date. The reason for the investigation will not be stated to Mid Kent ICT.

The employee or contractor will not necessarily be informed that an investigation is underway.

# Appendix E – Role descriptions and contact details

## Senior Risk Information Owner (SIRO).

The SIRO is the person nominated by the council to manage risk from a business, not a technical perspective.

Table 1 lists the SIROs for each of the Mid Kent Services partners.

*Table 1*

| Council | Name |
|---|---|
| **Maidstone Borough Council** | Mark Green |
| **Swale Borough Council** | David Clifford |
| **Tunbridge Wells Borough Council** | Lee Colyer |

## Data Protection Officer (DPO).

The DPO is responsible for overseeing data protection strategy and implementation to ensure compliance with GDPR.

Table 2 lists the DPO for each of the Mid Kent Services partners.

*Table 2*

| Council | Name |
|---|---|
| **Maidstone Borough Council** | Angela Woodhouse |
| **Swale Borough Council** | David Clifford |
| **Tunbridge Wells Borough Council** | Andy Sturtivant |