MALDON DISTRICT COUNCIL

Acceptable Use Policy

CONTEXT

We must act appropriately with the information we obtain and hold, and with the systems we use and access. How you use our systems, telephony, email and intranet is important for our reputation and the trust of our customers.

APPLICATION OF POLICY

Everyone who uses information and communications technology this organisation provides (or technology under any ownership used in the course of the business of this organisation) must be aware of these policy statements and the obligations it places upon them.

Maldon District Council commits to informing all employees, members, voluntary workers, agency staff, contractors and other third parties of their obligations before they are authorised to access systems and information and subsequently at regular intervals. Other organisations, and their users, granted access to technology managed by our organisation must abide by this policy.

All those who access information and communications technology may be held personally responsible for any loss or misuse.

OBLIGATIONS

- You must not install, access or modify applications, systems or data without the correct authorisation from IT.
- You must maintain the security of information as defined in the Information Security Policy.
- You must not access or interfere with other people's email without their permission, or in their absence, the authorisation of their line manager.
- You must not participate in unlawful, libellous, immoral or offensive activities, including accessing, downloading, storing, creating, copying or disseminating offensive material. This includes, but is not limited to, material of a pornographic, sexual, violent, criminal, racist, sexist or otherwise discriminatory nature. Further, you must not use our systems to perpetrate any form of fraud or piracy.
- You must not publish a website, or any content on a website or social media platform, that could bring the organisation into disrepute. This includes publishing defamatory or knowingly false material about the organisation, colleagues or customers in any online publishing format.
- You must not disclose your password to anyone or ask anyone else for their password. If you suspect your password has become known to anyone else, change it immediately and report this to ICT.
- Only subscribe to services with your professional email address when representing the organisation.
- Our facilities and identity must not be used for commercial purposes outside the authority or remit of this organisation, or for personal financial gain.

- You must not attempt to disable or bypass anti-virus, malware or other security protection, and you should take care not to introduce viruses or malware. If you discover a virus or malware, you must notify ICT immediately.
- You must only use software that is appropriately licensed and materials which are not copyrighted, or for which you have been granted use.
- You must only use council data for the purpose it was obtained and not to benefit yourself, a family member or friend
- If you receive or view email or other content not intended for you, protect its confidentiality.
- Take care when replying or forwarding to ensure that only relevant parties are included.
- Report faults with information and communications technology and co-operate with fault diagnosis and resolution.
- If you use our technology or our internet provision for personal use, the organisation takes no responsibility for the security of your personal information. It is recommended you do not carry out personal financial transactions.

MONITORING

The organization maintains the right to examine any system or device belonging to the organization in the course of our business, and to inspect any data held there. this includes but isn't limited to Laptops, tablets, phones and desktops.

To ensure compliance with this policy, the volume of Internet and network traffic, and the use and content of emails and visited Internet sites, is tracked and monitored. Specific content will not be monitored unless there is suspicion of improper use or required by a criminal investigation.

In regards to monitoring the user is question may be made aware of the monitoring event however this will be based on the situation at hand. If for example the monitoring was required due to a criminal investigation, the organization may be required to keep its findings confidential.

General ongoing non-descript monitor is run at all times for all organization devices.

For any specific request for Monitoring, CLT Approval is required prior to action taking place. If a request to monitor an individuate is made there has to be good cause for the request and specific information requested. All data is then kept secure and confidential in accordance with the Information security policy and only disclosed to the CLT for disclosure.

Where specific allegations of improper use are received relating to the conduct the individual will be informed of the allegations and the nature and scope of the investigation being undertaken in line with the relevant code of conduct policy.

FURTHER INFORMATION

Also see

Information Security Policy

Contact

Lead ICT Specialist

To report faults, contact

The ICT team on 01621 854477

To report a virus or malware, contact

The ICT team on 01621 854477

In the event of a password breach, or suspected breach, contact , Lead ICT Specialist, who acts as the Information Security Manager.