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 it to the Information Security Manager.
- 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 organisation maintains the right to examine any system or device used in the course of our business, and to inspect any data held there.

To ensure compliance with this policy, the volume of internet and network traffic, and the use and content of emails and visited internet sites, may be monitored. Specific content will not be monitored unless there is suspicion of improper use.

FURTHER INFORMATION

Also see

Information Security Policy

Contact

Chris Wall, ICT Manager

To report faults, contact

The ICT team on 875795 or 875770

To report a virus or malware, contact

The ICT team on 875795 or 875770

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

Information Security Policy

CONTEXT

Information is essential to delivering services to citizens and businesses. Information security refers to the defence of information or information systems from unauthorised or unintended access, destruction, disruption or tampering. It is important our organisation acts appropriately with the information we obtain and hold. Confidentiality, integrity and availability of information must be proportionate and appropriate to maintain services, comply with the law and provide trust to our customers and partners.

APPLICATION OF POLICY

Everyone who accesses information this organisation holds must be aware of these policy statements and their responsibilities in relation to information security.

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 information held by our organisation must abide by this policy.

All those who access information may be held personally responsible for any breach or misuse.

OBLIGATIONS

- Only access systems and information for which you are authorised.
- Only use systems and information for the purposes authorised.
- Comply with all applicable legislation and regulation.
- Comply with controls communicated by the Information Asset Owner.
- Do not disclose confidential or sensitive information to anyone without the permission of the Information Asset Owner.
- Ensure confidential or sensitive information is protected from view by unauthorised individuals.
- Do not copy, transmit or store information to devices or locations (physical or digital) where unauthorised individuals may gain access to it; the security of devices and locations you use are your responsibility.
- Protect information from unauthorised access, disclosure, modification, destruction or interference.
- Keep passwords secret and do not allow anyone else to use your access to systems and accounts (unless Maldon IT team require it to make updates)
- Notify the Information Security Manager of any actual or suspected breach of information security policy and assist with resolution
- Co-operate with compliance, monitoring, investigatory or audit activities in relation to information.

ROLES AND RESPONSIBILITIES

The Organisation

- Ensures compliance with law governing the processing and use of information.

The Chief Executive

- Acts as Accountable Officer ensuring that all information is appropriately protected.

Senior Information Risk Owner

- Assures information security within the organisation.
- Promotes information security at executive management level.
- Provides an annual statement about the security of information assets.

Information Security Manager

- Manages the investigation and mitigation of information breaches.
- Supports Information Asset Owners to assess risks and implement controls.

Information Asset Owners

- Assess the risks to the information they are responsible for.
- Define the protection measures of the information they are responsible for, taking consideration of the sensitivity and value of the information.
- Communicate the protection controls to authorised users and ensure controls are followed.

Directors, Managers and Line Managers

- Ensure their employees are fully conversant with this policy and all associated standards, procedures, guidelines and relevant legislation; and are aware of the consequences of non-compliance.
- Develop procedures, processes and practices which comply with this policy for use in their business areas.
- Ensure all contractors and other third parties to which this policy may apply are aware of their requirement to comply.

Employees

- Conduct their business in accordance with this policy.
- Take responsibility for familiarising themselves with this policy and understanding the obligations it places on them.

FURTHER INFORMATION

Contact

The ICT team on 875795 or 875770

In the event of an information breach, or suspected breach, contact Chris Wall, ICT Manager, who acts as the Information Security Manager.

Using Email and Digital Communications

CONTEXT

Email and digital communications are essential channels for our organisation, enabling us to work productively and flexibly.

How you communicate through email, instant messaging or audio-visual conferencing and what you publish on the internet is important for our reputation and the trust of our customers and partners.

Read the Information Security Policy and Acceptable Use Policy to understand your obligations.

AUDIENCE

This guidance is relevant for everyone who uses corporate email or digital communication channels in the name of Maldon District Council or acts as a representative of the organisation. It contains good practice and advice, describing the organisation's expectations as you use these channels.

All those who access email and digital communications may be held personally responsible for any abuse or inappropriate use.

CONTENTS

CHOOSING THE BEST CHANNEL

What do I need to communicate?

If information needs to be recorded or saved, or if you want to get a consistent message to a group of people, email is the answer. Short and insignificant conversation with somebody remote is ideal over instant messaging. Delivering an important, immediate and memorable message is best face to face, either in person or through video conferencing. For instant response combined with two-way dialogue, telephone remains a useful channel.

Channels for sensitive or complex subjects

If you are communicating about these matters, talk to somebody directly, or contact them using telephone or audio-video conferencing rather than email or instant messaging.

Performance appraisal or review issues | Job, salary or career progression

Topics which require discussion or dialogue | Private or privileged materials

Complex issues needing input from multiple people | Venting frustration

This ensures that aural or visual cues are evident in the conversation. Of course, you may need to follow up dialogue with documented notes or information, at which time email becomes an acceptable channel.

EMAIL ETIQUETTE

Keep emails short and to the point. The people receiving your email want to quickly understand how they should prioritise your message. Long emails may not be read to the end.

Use the subject field for a brief and concise description or reference. This helps the recipient organise and manage their email and will help you retrieve it if needed.

Read your email back to yourself before you send it, as it lets you check you are conveying the message you want, as well as correcting spelling or grammar mistakes which shows respect for the intended audience.

Do you need to attach something? When referring to other information or documents, think about whether the recipient can access a link rather than sending an attachment. This reduces the strain on your mailbox storage and theirs. It also reduces duplication as it discourages multiple copies being saved, and ensures the original information remains the key reference location.

Say Hello, Goodbye and who you are. Use a salutation appropriate for your audience. It is common practice to use Hi or Hello in professional emails, or to use Dear in particularly formal emails. Finishing your email with "Kind regards" or "Thanks" above your signature helps to stop communication feeling abruptly closed. Include a signature that provides enough information about who you are without making it unreasonably long. A corporately agreed disclaimer is automatically added to external emails therefore do not add your own version of a disclaimer to your signature.

Avoid snap responses. Never send an email in anger. Email can be very impersonal so it may encourage people to feel bolder in making criticism or pointing out things they are dissatisfied with than they would be in communicating it verbally. Whilst it may be tempting to respond in kind, it is always better to wait until your initial irritation is gone and then either speak to them in person or construct a considered response.

MANAGING EMAIL

Don't let email overwhelm you by setting a little time aside each day to deal with it. Consider whether senders need you to respond, retain or just read then delete. Use flags and reminders for emails which require a response you cannot immediately provide. Empty the deleted items folder intermittently and archive old items in your mailbox regularly to prevent it becoming unusable.

If you are able to work flexibly or remotely, you may collect email on your mobile phone or online. As technology enables us to work from almost anywhere with an internet or phone connection, it can be difficult to know where to draw the line. The relaxation of traditional work boundaries can cause feelings of pressure on your work life balance and difficulty switching off from work.

You are not expected to read and answer emails outside your normal working hours. Urgent matters can be communicated by telephone. There is no expectation you are always available just because you have connectivity.

Avoid peer pressure and do not get involved in competitive situations over email responses.

Be considerate of the time and day when sending emails. If you manage others, you should avoid setting an expectation that your team need to work when you work.

Set an out-of-office response when you are unable to read your emails for at least one working day or more. This helps to manage the expectations of those contacting you.

You do not need to check emails when you are off sick, on holiday or non-working days, but you should ensure they are managed on your behalf or that senders have an alternative point of contact.

You are responsible for managing your work time. Look for early signs of email invasion into your personal time and act quickly.

SENSITIVITY

Give some thought to whether a message needs to be marked differently to usual. Most messages and their attachments don't need to be marked as confidential or private, and when they aren't, the assumption is that the message can be forwarded and the attachment changed as required. Please do not use auto-forward rules on your emails as this restricts your ability to manage them according to their sensitivity.

Most email applications make it easy to mark emails with a sensitivity level. If in doubt, start your subject line with the appropriate word to indicate sensitivity. Be aware that marking with a sensitivity level does not prevent recipients distributing the content.

Remember privacy and confidentiality cannot be assured on most digital channels. Secure email should be used for sensitive information about individuals, or is sensitive due to quantity (e.g. large datasets of personal details) or content which is commercial in confidence.

Confidential messages and attachments should not be freely copied or forwarded. Distribution should be limited to those who need to be informed.

Private indicates the content is only to be shared between the sender and recipient. The recipient should seek the sender's permission before distributing or sharing the information.

Marking digital correspondence with **Personal** tells the recipient that the content is about the sender. The recipient should seek the sender's permission before distributing or sharing.

DIGITAL COMMUNICATIONS AND THE LAW

The law applies to email and digital communications in the same way as it does to the written or spoken word, regardless of intent or ignorance. Think carefully about what you say and how you say it. The organisation will assist law enforcement agencies when requested, including passing on all data held on email.

The law of copyright applies to electronic and digital forms in the same way as it does to traditional publications. Take care not to infringe copyright when reproducing any material in email, attachments or digital communications. Seek advice from Legal Services if you are unsure.

Everything contained in the email system is the organisation's intellectual property.

Data Protection and Freedom of Information

It is a criminal offence to collect, hold and process personal data on computers unless the Information Commissioner's Office is notified. This organisation is registered as a data processor. Information held in emails about a person may have to be revealed if they request it. Be mindful that email is included in the information subject to disclosure under the Freedom of Information Act 2000. It is also a legal requirement that information held is accurate and is only kept for as long as it is needed.

Human Rights Act 1998

Article 8 of this Act applies to emails and digital correspondence sent at work and gives individuals the right to privacy over such communications. However, monitoring individuals' email and digital correspondence at work may be justified if it is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety, for the economic wellbeing of the country, for the prevention of disorder or crime, for protection of health or morals or for the protection of the rights and freedoms of others.

Obscene Publications Act 1959 and 1964

Material sent through the email system or shared digitally during working time or from the organisation's equipment could contravene this act, and information will be passed to appropriate authorities if requested.

Defamation

Critical comments or defamatory remarks about individuals, groups or organisations must not be included in corporate email or shared through digital channels when acting as a representative of the organisation. You must not reproduce any critical comments or defamatory remarks made by third parties as the law may interpret this as libel and you may be held liable for the contents.

Harassment and Discrimination

Comments or remarks sent by email or shared digitally may amount to harassment under anti-discrimination laws. Because there are no visual or tonal signals in digital communications, it is possible to cause offence to the recipient or reader where none was intended.

Contracts

It is possible to inadvertently form a contract through an exchange of email. A contract does not necessarily need a signature to come into force, and in any event, your email signature has the same weight in law as your manuscript signature. If you do not have the authority to create or vary a contract, take care in your email correspondence, and seek advice from Legal Services if needed.

Hacking

Unauthorised access to our network or systems, including email, can lead to theft, destruction or alternation of essential data. It is a criminal offence to access any computer system you are not authorised to use, or to delete or amend data or systems to the detriment of the organisation.

REPORTING EMAIL OR DIGITAL COMMUNICATIONS

Abusive or Obscene Content

Make sure you know and understand your obligations around inappropriate and unacceptable communications: see the Acceptable Use Policy. If you are unsure as to whether email or digital communication content could be offensive, do not send or share it. Remember you represent our organisation in all communications and should not do anything to bring it into disrepute.

Abusive or obscene content is not defined by what you consider abusive or obscene; it is what anyone could find to be abusive or obscene.

If you receive offensive material by email from an unknown source, do not reply or participate in any way as this may confirm to the sender that your email address exists and lead to further unwanted email. Inform your line manager and ICT.

If you receive offensive material from a known source, request they stop this in future and please tell your manager. You may notify ICT if you choose.

Viruses and Malware

Anti-virus and anti-malware tools are used throughout our network. Nonetheless some suspicious communications may find their way to you by masking themselves as a trusted correspondent or domain, or by being inconspicuous enough to avoid detection. Think carefully before opening attachments or following links you weren't expecting. Delete suspicious emails straight away, notifying the sender by separate email (not by replying) if you think there was a chance of authenticity. If you mistakenly open an attachment or follow a link which proves to be bogus, notify ICT immediately who will try to limit any issues; stop working on your PC or mobile device and do not attempt to remove any virus or malware yourself.

FURTHER INFORMATION

Also see **Information Security Policy, Acceptable Use Policy**

Contact Chris Wall, ICT Manager

To report concerns, contact the ICT team on 875795 or 875770