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.

Senior ICT Specialist

- Assures information security within the organisation.
- Promotes information security at executive management level.
- Provides an annual statement about the security of information assets.
- Supports Information Asset Owners to assess risks and implement controls.

Senior Legal Specialist

- Manages the investigation and mitigation of information breaches.
- 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 01621 854477

In the event of an information breach, or suspected breach, contact Grant Hulley, Senior ICT Specialist, who acts as the Information Security Manager.