|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Title:** | **(ICT) Security Policy** | | | | **Milton Keynes Council logo** |
| **Number:** | |  | **Version:** | 2.3 | **Council policies and procedures manual** |

|  |  |  |  |
| --- | --- | --- | --- |
| **Version History** | | | |
| **Version** | **Date** | **Detail** | **Author** |
| 2.0 | 1/4/15 | First Draft | Paul Wheeler |
| 2.1 | 30/6/15 | Updated with feedback comments from Corporate IT group | Paul Wheeler |
| 2.2 | 08/05/18 | Update branding and incorporate GDPR | Paul Wheeler |
| 2.3 | 1/11/19 | Include Cyber Security conditions | Paul Wheeler |
|  |  |  |  |
|  |  |  |  |

Contents

[1 Policy Statement 2](#_Toc424116959)

[2 Purpose 2](#_Toc424116960)

[3 Scope 2](#_Toc424116961)

[4 Definitions and Responsibilities 2](#_Toc424116962)

[5 Risks 3](#_Toc424116963)

[6 Applying the Policy 3](#_Toc424116964)

[6.1 Authorised Use 4](#_Toc424116965)

[6.2 Acceptable use 4](#_Toc424116966)

[6.3 Security awareness 4](#_Toc424116967)

[6.4 Business Continuity 4](#_Toc424116968)

[6.5 Monitoring and reporting 4](#_Toc424116969)

[6.6 Risk Assessment 5](#_Toc424116970)

[6.7 Security Policy Review 5](#_Toc424116971)

[6.8 Asset Management 5](#_Toc424116972)

[6.9 Sanctions and Disciplinary Action 5](#_Toc424116973)

[7 Policy Compliance 5](#_Toc424116974)

[8 Compliance with legal and contractual obligations 5](#_Toc424116975)

[9 Development of specific ICT policies, procedures and guidelines 6](#_Toc424116976)

[10 Breaches of Policy 6](#_Toc424116977)

[11 Incident Reporting 6](#_Toc424116978)

[12 Incident Management 6](#_Toc424116979)

[13 Policy Governance 7](#_Toc424116980)

[14 Review and Revision 7](#_Toc424116981)

[15 Key Messages 7](#_Toc424116982)

[16 Appendix A- List of Milton Keynes Council Policies 8](#_Toc424116983)

# Policy Statement

This policy is the council’s approach to Information and Communications Technology (ICT) Security Management and contains no sensitive or restricted information and may be freely publicised to relevant parties.

# Purpose

Milton Keynes Council has a large investment in the use of Information Technology (IT) and Telecommunications which is used to the benefit of all departments. These resources are funded from public money and are provided to enable the Council to carry out its business in providing services to the people of Milton Keynes. In many areas of work the use of IT is vital and must be protected from any form of disruption or loss of service including the loss of data through Cyber attacks. It is therefore essential that the availability, integrity and confidentiality of the IT systems and data are maintained at a level which is appropriate for the Council’s needs

# Scope

This ICT Security Policy applies to, but not limited to all Milton Keynes Council Councillors, Committees, Departments, Partners, Employees of the Council, contractual third parties and agents of the Council who access the Councils systems and process data on behalf of the Council:

* ICT systems belonging to, or under the control of, Milton Keynes Council;
* Information stored, or in use, on Council ICT systems;
* Information in transit across the Council’s voice or data networks;
* Control of information leaving the Council;
* Information access resources;
* All parties who have access to, or use of ICT systems and information belonging to, or under the control of, Milton Keynes Council including:

Application of this policy applies throughout the information lifecycle from acquisition to disposal.

# Definitions and Responsibilities

Co-ordination:

The Council co-ordinates information technology security policy across the authority through the following roles:

* Head of Strategic ICT Development:
* Senior Information Risk Owner (SIRO):
* IT Security Officer (ITSO):

Any concerns may be addressed directly to the above, reported via the IT Service Desk or communicated as an agenda item on the monthly Corporate ICT Group.

* IT Security Officer: The Council’s IT Security Manager is responsible for ensuring policies and procedures are in place to cover all aspects of ICT systems and Information security. All policies will be communicated across the Council to ensure good working practices and to minimise the risk to the Council’s reputation.
* Corporate Directors, Service Directors, Heads of Service, Assistant Directors: are responsible for ensuring that ICT systems and information within their service areas are managed in accordance with the Council’s ICT Security Policy. Day to day responsibility for the management of ICT systems and information may be delegated to staff designated system owners within departments.
* Users: It is the responsibility of any individual or organisation having access to the Council’s ICT systems and information to comply with the Council’s ICT Security Policy, associated guidelines and procedures and to take adequate steps to safeguard the security of the ICT systems and information to which they have access. Any suspected or actual security weakness, threats, events or incidents must be immediately reported to the ICT Service desk or any of the ICT Security Co-ordination roles above.

# Risks

Milton Keynes Council recognises that there are risks associated with users accessing and handling information in order to conduct official Council business.

This policy aims to mitigate the following risks:

* Unauthorised access to information
* Unauthorised introduction of malicious software and viruses.
* Potential sanctions against the Council or individuals imposed by the Information Commissioner’s Office as a result of information loss or misuse
* Potential legal action against the Council or individuals as a result of information loss or misuse
* Council reputational damage as a result of information loss or misuse.

Non-compliance with this policy could have a significant effect on the efficient operation of the Council and may result in financial loss and an inability to provide necessary services to our customers.

# Applying the Policy

The Council is committed to the development and maintenance of an ICT Security Policy to:

* Provide direction and support for ICT security in accordance with business requirements, regulations and legal requirements;
* State the responsibilities of staff, partners, contractors and any other individual or organisation having access to the Council’s ICT systems;
* State management intent to support the goals and principles of security in line with business strategy and objectives.
* Provide a framework by which the confidentiality, integrity and availability of ICT resources can be maintained.
* Optimise the management of risks, by preventing and minimising the impact of ICT security incidents;
* Ensure that all breaches of ICT security are reported, investigated and appropriate action taken where required;
* Ensure that supporting ICT security policies and procedures are regularly reviewed to ensure continued good practices and protection against new threats;
* Ensure ICT information security requirements are regularly communicated to all relevant parties.

## Authorised Use

Access to ICT systems and Information for which the Council is responsible is permitted in support of the Council’s areas of business or in connection with a service utilised by the Council. Authorised users are defined as: Council employees, elected members, authorised contractors, temporary staff, partner organisations or members of the public when using public information services provided by the Council.

## Acceptable use

All users of ICT systems and information for which the Council is responsible must agree to and abide by the terms of this policy and associated security policies and applicable Codes of Connection or Conduct.

## Security awareness

The Council is committed to promoting safe working practices. It is the responsibility of managers to ensure that users of resources have the appropriate training commensurate with the information and systems to which they have access. Relevant information security policies, procedures and guidelines will be accessible and disseminated to all users. It remains the employees’ responsibility to ensure they are adequately informed of information technology security policies and procedures . Everyone, from our customers and partners to our employees and contractors, should feel that their data is safe. The only way to gain their trust is to proactively protect our systems and databases. We can all contribute to this by being vigilant and keeping cyber security top of mind.

## Business Continuity

The Council has developed, and maintains, a Business Continuity Strategy based on specific risk assessment to maintain critical business functions including ICT in the event of any significant disruption to services or facilities on which the Council is reliant.

## Monitoring and reporting

The Council reserves the right to monitor the use of ICT systems and information, including email and internet usage, to protect the confidentiality, integrity and availability of the Council’s information assets and ensure compliance with the Council’s policies. The Council may, at its discretion, or where required by law, report security incidents to the relevant UK authorities for further investigation.

## Risk Assessment

The Council has developed a Risk Management Strategy and the risk to the Council’s ICT systems and information will be managed under this framework with reference to the guidelines detailed in *BS 7799-3:2006 Information security management systems – Part 3: Guidelines for information security risk management.* Reviews are independent, unbiased and verified by either internal audit or external parties when required.

## Security Policy Review

The Council will conduct an annual review of the policy or following any significant security incidents by any parties under section 2, changes to UK or EU legislation or changes to the Council’s business requirement or structure.

## Asset Management

The Council or its agents will maintain an inventory consisting of all information assets which will be managed in accordance with the Council’s information security policies and procedures.

## Sanctions and Disciplinary Action

Failure of Council employees to comply with the Council’s Information Security Policy may lead to disciplinary action under the Council’s disciplinary procedure.

Failure of contractors, temporary staff, public, partners or third party organisations to comply with the Council’s Information Security Policy may result in termination of contracts and connections, suspension of services and/or lead to prosecution.

# Policy Compliance

If any user is found to have breached this policy, they will be subject to Milton Keynes Council’s disciplinary procedure. If a criminal offence is considered to have been committed further action may be taken to assist in the prosecution of the offender(s).

We expect all our employees to always follow this policy and those who cause security breaches may face disciplinary action:

* First-time, unintentional, small-scale security breach: We may issue a verbal warning and train the employee on security.
* Intentional, repeated or large-scale breaches (which cause severe financial or other damage): We will invoke more severe disciplinary action up to and including termination.

We will examine each incident on a case-by-case basis.

Additionally, employees who are observed to disregard our security instructions will face progressive discipline, even if their behaviour hasn’t resulted in a security breach.

# Compliance with legal and contractual obligations

Milton Keynes Council will abide by all UK legislation relating to information processing including:

* General Data Protection Regulation 2016
* The Data Protection Act (2018)
* The Freedom of Information Act (2000)
* The Computer Misuse Act (1990)
* The Human Rights Act (1998)
* The Copyright, Designs and Patents Act (1988).
* The Regulation of Investigatory Powers Act (2000)
* The Electronic Communications Act (2000)
* Privacy and Electronic Communications Regulations (2003)

Milton Keynes Council will also comply with any contractual requirements, standards and principles required to maintain the business functions of the Council including:

* Protection of intellectual property rights;
* Protection of the authority’s records;
* Compliance checking and audit procedures;
* Prevention of facilities misuse;
* Relevant codes of connection to third party networks and services.

# Development of specific ICT policies, procedures and guidelines

The Council is committed to the ongoing development and review of ICT policies, procedures and guidelines to manage the risk of emerging threats to its systems and services. Any major revisions of the policy will be presented at the monthly Corporate ICT Board and will need to be agreed by the ITSO, SIRO and Head of Strategic ICT Development.

# Breaches of Policy

Breaches of this policy and/or security incidents can be defined as events which could have, or have resulted in, loss or damage to Council assets, or an event which is in breach of the Council’s security procedures and policies.

All Council employees, councillors, partner agencies, contractors and vendors have a responsibility to report security incidents and breaches of this policy as quickly as possible through the Council’s Incident Reporting Policy. This obligation also extends to any external organisation contracted to support or access the Information Systems of the Council

The Council will take appropriate measures to remedy any breach of the policy and its associated procedures and guidelines through the relevant frameworks in place. In the case of an individual then the matter may be dealt with under the disciplinary process.

# Incident Reporting

Under the council’s Incident Reporting Policy, all breaches must be reported at the earliest opportunity by the person discovering the breach. Breaches can involve not only Information Technology equipment but also data that is mishandled, lost or abused or any other incident which may cause a security concern or which may contravene the Council’s IT Security Policy, Data Protection Policy and/or any other associated policies.

# Incident Management

During reporting of a breach, details of the incident will be entered into the call logging system by the IT Service Desk operator taking the call. Once the call has been entered into the system, an email will be sent to the IT Security Officer, Head of Strategic ICT Development and the council’s SIRO. The aforementioned officers (either individually or collectively) will then determine escalation path and any representations or reporting which has to be made to the Information Commissioner’s Office, law enforcement, internal audit or any other agency.

# Policy Governance

The following table identifies who within Milton Keynes Council is Accountable, Responsible, Informed or Consulted with regards to this policy. The following definitions apply:

* Responsible – the person(s) responsible for developing and implementing the policy.
* Accountable – the person who has ultimate accountability and authority for the policy.
* Consulted – the person(s) or groups to be consulted prior to final policy implementation or amendment.
* Informed – the person(s) or groups to be informed after policy implementation or amendment.
* Responsible Senior Information Governance Officer
* Accountable Data Protection Officer
* Consulted Knowledge and Information Services Steering Group
* Informed All Staff, Councillors, Contractors and Partners

# Review and Revision

This policy will be reviewed as it is deemed appropriate, but no less frequently than every 12 months.

Policy review will be undertaken by the Information Assurance Governance Manager.

# Key Messages

Users must familiarise themselves with the detail, essence and spirit of this policy before using the IT Systems of the Council provided.

Users are responsible for ensuring the security of their network account logon-id and password.

Users must assess any risks associated with processing of data and ensure that the work practices being employed are the most appropriate mechanism to use

# Appendix A- List of Milton Keynes Council Policies

| **Title** | **Status** | **Review Date** |
| --- | --- | --- |
| Information Processing Policy | Revised May 2018 |  |
| Incident Reporting Policy | Revised May 2018 |  |
| Acquisition and disposal of ICT Equipment Policy | Revised May 2018 |  |
| Social Media Policy | Revised May 2018 |  |
| Mobile and Fixed Line Telephony Policy | Revised May 2018 |  |
| Physical Access Policy | Revised May 2018 |  |
| Patching Management Policy | Revised May 2018 |  |
| Agile Working Policy | Revised May 2018 |  |
| Data Protection Policy | Revised May 2018 |  |
| Internet Acceptable Use Policy | Revised May 2018 |  |
| Email Acceptable Use Policy | Revised May 2018 |  |
| Password & System Access Policy | Revised May 2018 |  |
| Clear Desk Policy | Revised May 2018 |  |
| Cyber Security and awareness | October 2019 |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |