APPENDIX C

Title: # Email policy		milton keynes council
Number:	**Version:** 1.4	**Council policies and procedures manual**

Contents

1. Policy Statement

This policy sets out how Milton Keynes Council (MKC) uses email facilities for communication, as well as expectations about how the information sent and received is to be managed. It supports the wider information governance and security agendas.

2. Scope

This policy applies to all employees, councillors, contractors and volunteers working for, or on behalf of, Milton Keynes Council. It covers communications with both internal and external parties.

3. Definition

This Email Usage Policy should be applied at all times whenever using the Council provided Internet facility. This includes access via any access device including a desktop computer or a smartphone / tablet device

4. 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.

5. Applying the Policy

5.1 The role and status of email

Email is a business tool for both internal and external communication. All email messages, both sent and received, are documents of the Council. They have the same status in law as written correspondence (letters and faxes etc.), and are subject to the same legal implications.

This means that they may need to be disclosed in response to requests for information under the Freedom of Information Act 2000, Environmental Information Regulations 2004, or as part of legal proceedings. The laws relating to libel, defamation, and discrimination etc. also apply to the content of email messages. Further action could result from inappropriate content.

5.2 Mailbox Management

Email systems are not suitable for long term document management. Messages should only be managed in email applications for a short period before being either **deleted or transferred** to a line-of-business system application, document management system, or a managed file share or shared mailbox like any other business document.

Data should not be held for longer than is necessary for the purpose. In order to comply with legislation it is imperative that unwanted emails are deleted. As a baseline the following controls will be implemented:

- **All mail not managed into a shared mailbox, application or file share and has exceeds the 12 month retention period agreed by CLT will be deleted after 12 months.**

5.3 Personal use

Personal use of the email system is no longer permitted. Email addresses are increasingly being targeted by cyber criminals and using your council email address outside of work purposes puts us at greater risk of being included in a cyber-attack. The previous policy was put in place before people had access to personal email on their own devices and before cyber-attacks were as prevalent as they are today. This policy change reflects the times we live in now and ensures that we lower the risk of the council being targeted by cyber criminals.

Access to personal email is now generally available on personal devices and the Council provides free Wi-Fi access in key buildings.

Forwarding of chain mail is not permitted.

Where MKC email facilities are used to send or receive messages, for whatever purpose, the Council remains the data controller for the information contained. This means that the content may be subject to legislative compliance. Care must therefore be taken not to bring the Council into disrepute in any way. As a result of this measure No automated rules to redirect corporate email to non-corporate (Non-Milton Keynes Council) email addresses is permitted as this would breach the security principles outlined under GDPR.

5.4 Security and resource management

MKC takes the security of its network and the wellbeing of staff seriously. A range of security measures are in place to protect the interests of the Council, staff, and customers.

The Council reserves the right to monitor email messages and email usage. This is done to:

- enable the organisation to manage the resources effectively.
- enable the organisation to plan appropriately for future requirements.
- implement filtering to detect and remove dangerous and inappropriate content.
- support the detection and prevention of crime.
- support investigations of inappropriate and unauthorised use.

A warning message is displayed during network login to remind users of the monitoring activities.

Standard email messages are secured using encryption (TLS 1.2). Care should be taken over the content of messages sent via email to minimise the risk of exposing sensitive information. Tools are available to improve the security of messages when this is required. Contact the IT Servicedesk for advice on appropriate approaches.

5.4.1 Scanning and filtering

In addition to legitimate business email messages the organisations email systems receive messages that are unwanted, and in some cases dangerous. These include:

- Emails containing viruses.
- Emails containing harmful content e.g. script exploits.
- Emails containing inappropriate material e.g. pornographic images.
- Emails which are otherwise unwanted (SPAM).

Both incoming and outgoing messages are scanned to detect unwanted or inappropriate content. The actions taken when such content is detected include:

- Notifying relevant staff.
- Quarantining for further analysis.
- Cleansing – removal of the problem content when this is possible.
- Deletion of the message.

Some of the filters block incoming messages on the basis of the source of the message. If you are expecting an email from a new source that hasn't arrived the IT Helpdesk will be able to advise whether the message might have been blocked, and make appropriate arrangements to allow its delivery.

5.4.2 Legal disclaimer for outgoing messages

A legal disclaimer is automatically appended to all outgoing email messages. In addition this message contains a link to the MKC website, and encouragement not to print the email unnecessarily. The message does not appear in the sent message as stored by the email system.

5.4.3 Email account quotas

Quotas will be applied to email accounts limiting the amount of storage space available.

5.4.4 Secure email

Secure email facilities, which encrypt messages for transmission, are available for communicating with external parties. They should be used when the message, including any attachments, contains sensitive personal details or information that is confidential for business reasons. If there is any doubt about the requirement, err on the side of caution and use a secure email facility.

For further information or to request access to the secure email facility, contact MKC IT.

5.4.5 Use of non-work email accounts/addresses

Email accounts not provided by MKC must not be used for sending or receiving business email. Corporate email that contains personal or business confidential data must not be forwarded to private email accounts.

5.5 Administration of email facilities

The ICT Service is responsible for operational management of the email facilities. All enquiries and requests should be made via the IT Helpdesk.

5.6 Training

MKC will provide training for all staff to support them in making appropriate and effective use of email communication.

All staff are encouraged to take advantage of the training that is available, and to identify any unmet needs for discussion as part of the appraisal process.

6. Acceptable Usage Policy

Each user must read, understand and verify they have read and accepted this policy.

7. Responsibilities

Party	Key responsibilities
Information Governance Group	Ensure that this policy is monitored and continues to be relevant.
ICT	Operational management and monitoring of email facilities.

8. 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).

If you do not understand the implications of this policy or how it may apply to you, seek advice from your line manager.

9. 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 Risk Officer
Accountable	Data Protection Officer
Consulted	Corporate IT Group, Information Governance Board
Informed	All Staff, Councillors, Contractors and Partners

10. 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.

11. References

1 Data Protection Act 2018. GDPR (2016)

2 Freedom of Information Act 2000. (c. 36), London: HMSO.

3 Environmental Information Regulations 2004. SI 2004/3391, London: HMSO

4 Managing email (CPIG110).

5 Writing business emails (CPIG120).

12. Key Messages

Users must familiarise themselves with the detail, essence and spirit of this policy before using the email facility provided.