MANCHESTER CITY COUNCIL

Introduction to the Internet & Email Policy

E-mail and internet are important business communication tools, and widely accepted as the most efficient way to make contact with, or stream information to others.

The Internet and Email Policy (I&EP) is one of the Council's most vital policies. It supports our Information Security Policy and its Code of Practice, which are based on the British and International Standards for Information Security, and comply with all relevant legislation and best practice guidance provided by the Information Commissioners Office (ICO) and other government agencies.

The I&EP includes guidance, regulations and conditions of use, and it also sets out our responsibilities. The key thing to remember is that email and internet use is subject to the same business, legislative and accountability standards as printed and verbal communications: we all need to stick to the rules and expect everything that we do by email or online to be subject to the same scrutiny as more traditional communications.

Possibly the most important detail is the section about online safety and keeping sensitive information safe. We should all be aware of the Internet Security Code of Practice, and understand that there are vulnerabilities in even the most robust systems, so our day to day practice needs to be mindful of any potential lapse.

Within this Policy there are sections relating to:

Aims

Setting out why we need this policy, who it applies to and what it hopes to achieve.

Information Security

Detailed section focussed on our duty to protect the information we keep, prevent the unauthorised sharing of information, and prohibited use of the internet and email.

Passwords

Outline of the protocol for passwords, and how to keep them safe.

Filtering software

To uphold our responsibility for protecting information, we filter all incoming and outgoing information.

Access

Guidance on giving access to your email.

Monitoring

Statement about monitoring of internal/external communications, including situations in which monitoring is authorised, why and how the detail is stored for future use e.g.: investigations or complaints.

Individual/shared accounts

Setting out why colleagues may need access to your account and how / when to do this properly. Also detail about why it's important not to share without the proper authority.

Archiving

The storing of information and what it can be used for.

Internet/intranet

Outline of appropriate use of each.

Personal use

Guidelines for personal use, limits and standards of behaviour. Also details our responsibility to report unauthorised personal use that breaches any of the guidelines e.g.: excessive, discriminatory, offensive or racist.

Email protocol

Looks at content and language, and disclosure of information.

Encryption

When this can and should be used and the potential consequences of failing to encrypt information that's emailed.

Sensitive/protected information: incoming and outgoing, internal and external.

This section of the policy is essential reading for all employees: we all need to understand data protection legislation to the extent that it applies to each of us when sharing information. Includes detail about reporting inappropriate sharing of sensitive information, intentional or accidental.

Please take the time to read through the Internet & E-mail Policy: much of its content is common sense and you may consider yourself to be fully aware of the rules, regulations and potential pitfalls.

But the risk of making mistakes, leaving the entire organisation open to criminal activity is very real, so protect us all by protecting yourself.