Report of the Service Directors
Asset Management and Culture and
Human Resources

Decision to be taken after:
8 March 2010

NORTH LINCOLNSHIRE COUNCIL

CORPORATE SERVICES CABINET MEMBER

INTERNET AND EMAIL ACCEPTABLE USE POLICIES

1. OBJECT AND KEY POINTS IN THIS REPORT

1.1 To seek approval to formally adopt the proposed North Lincolnshire Council Internet and Email acceptable use policies.

1.2 Key points in this report are as follows:

- The council wide use of the NLC Internet and Email facilities
- Previous misuse of the facilities
- The need for up to date enforceable policies
- Future circulation and awareness of the policies

2. BACKGROUND INFORMATION

2.1 Internet access and the Lotus Notes email system were first introduced across the council in 1999. Initially this was limited, however over subsequent years the widespread use and reliance on the facilities has increased dramatically.

2.2 Following the initial introduction of the facilities, guidelines on the correct use of the systems were written and circulated, but not formally adopted as council policy.

2.3 The Internet and Email system is used by over 2,500 officers and elected members, and is now also available through mobile devices such as Blackberries.

2.4 As the Internet and websites have developed, many other innovative functions and facilities are becoming available. In recent years the growth of social media/networking websites (i.e. Facebook, YouTube, MySpace) has resulted in this category becoming the largest global use of the Internet. The council requires a fit for purpose policy to ensure that all employees are aware of the acceptable use of the facilities available to them. These policies advise individuals and line managers of the correct use.

2.5 Over the last five years, a number of investigations have taken place relating to the potential misuse of the North Lincolnshire Council Internet and Email systems, some of which have resulted in formal disciplinary action.

2.6 A new software system called Policy Matters was recently introduced to distribute policies to all North Lincolnshire Council officers and members. This system will enable Human Resources and IT Services to monitor and report on the status of officers understanding and accepting the contents of the policies.

3. OPTIONS FOR CONSIDERATION

3.1 The following options are available for the Cabinet Member to consider.

3.1.1 **Option1 -** To consider and adopt the Internet and Email acceptable use policies. Distributing and embedding the policies via the Policy Matters system and through a promotion programme consisting of notice board posters and Intralinc publicity.

3.1.2 **Option 2** - To reject the proposed Internet and Email acceptable use policies.

3.1.3 **Option 3 -** To make recommendations to amend the proposed policies.

4. ANALYSIS OF OPTIONS

4.1 The proposed policies were produced to reflect the experiences of Human Resources and Internal Audit with regards to misuse. The consideration and adoption of the policies would ensure that all IT users are aware of the contents and the need for adherence.

4.2 Rejecting the proposed policies could result in the council’s approach to the use of these facilities not reflecting current practices within other local authorities and government bodies. This could also result in the misuse of council assets and resources.

4.3 Recommending further changes to the procedure would require further consultation and delay the final implementation.

5. RESOURCE IMPLICATIONS (FINANCIAL, STAFFING, PROPERTY, IT)

5.1 There are no direct financial, staffing or property implications arising from this report.

5.2 **IT**

An existing system (Policy Matters) will be used to distribute the Policies.

6. OTHER IMPLICATIONS (STATUTORY, ENVIRONMENTAL, DIVERSITY, SECTION 17 - CRIME AND DISORDER, RISK AND OTHER)

6.1 None

7. OUTCOMES OF CONSULTATION

7.1 The trade unions were consulted via the Corporate Consultative Group and are fully supportive of the new policies. The IT Strategy Board, HR, Internal Audit and IT Services were also consulted and contributed to and support the proposed policies.

8. RECOMMENDATIONS

8.1 That the Cabinet Member approves the new Internet and Email Acceptable Use policies for adoption across the council.

SERVICE DIRECTOR ASSET MANAGEMENT AND CULTURE
SERVICE DIRECTOR HUMAN RESOURCES

Pittwood House
Ashby Road
Scunthorpe
DN16 1AB
Author: R Bulmer/M Oglesby
Date: 12th February 2010

Background Papers used in the preparation of this report:

- The current Internet and Email guidelines.

Internet Acceptable Use Policy

NORTH
LINCOLNSHIRE
COUNCIL

IT Services

Asset Management and Culture

Internet Acceptable Usage Policy

CONTENTS

1. Purpose of the Policy

1.1 This policy document informs you how to use your North Lincolnshire Council Internet facility. It outlines your personal responsibilities and defines what you must and must not do.

1.2 The Internet facility is made available for the business purposes of the Council. A certain amount of personal use is permitted in accordance with the statements contained within this Policy. It is recognised that it is impossible to define precise rules covering all Internet activities available and adherence should be undertaken within the spirit of the policy to ensure productive use of the facility is made.

1.3 This policy replaces the Council's Internet and Email Guide.

1.4 This Internet Acceptable Use Policy applies to, but is not limited to, all North Lincolnshire Council's Members, Committees, Departments, Partners, Employees of the Council, school employees and teaching staff, contractual third parties and agents of the Council who access the Councils Internet service and IT equipment. Public Internet access i.e. Libraries, are excluded from this policy.

1.5 This Internet Acceptable 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/notebook computer or a Smart phone device.

2. Internet risks

2.1 North Lincolnshire 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:

- *Exposure to inappropriate material*
- *Security compromises from virus/Trojans or spy ware*
- *Risks to children through inappropriate content, contact or conduct*

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

3. Safeguarding Children

3.1 The Council is committed to keeping children safe within North Lincolnshire and as part of this commitment it promotes the ethos that safeguarding children is everybody's business. The Internet is another tool by which a child could be harmed. The Council is committed to ensuring that within the organisation the Internet is used to enhance working practice and not to be misused in a way that can harm children and young people. The Council operates the Managing Allegations Against People who work with Children (LADO) procedures and this policy should be read in conjunction with these procedures.

3.2 The LADO procedures outline the action that will be taken when there are concerns raised regarding someone's suitability to work with children, with regard to this policy it will specifically relate to concerns regarding contact, conduct or content on the Internet by people who work with children.

4. Applying the Policy

4.1 What is the Purpose of Providing the Internet Service?

The Internet service is primarily provided to give Council employees and Members:

- *Access to information that is pertinent to fulfilling the Council's business obligations.*
- *The capability to post updates to Council owned and/or maintained web sites.*
- *An electronic commerce facility.*

4.2 What You Should Use Your Council Internet Account For

Your Council Internet account should be used in accordance with this policy to access anything in pursuance of your work including:

- *Access to and/or provision of information.*
- *Research.*
- *Electronic commerce (e.g. purchasing equipment for the Council).*

4.3 Personal use of the Council's Internet Service

Provided it does not interfere with your work, the Council permits personal use of the Internet in your own time, for example during your lunch-break. (Ref 4.5)

Staff working on PCs in front-line locations must not access the Internet for personal reasons at any time when members of the public are (or could be) present, regardless of whether their personal working pattern has yet to start or has been completed. This restriction applies particularly to front line staff in Libraries and Leisure Centres, etc

The Council is not, responsible for any personal transactions you enter into (i.e. in respect of the quality, delivery or loss of items ordered). You must accept responsibility for, and keep the Council protected against, any claims, damages, losses or the like which might arise from your transaction (i.e. in relation to payments for the items or any personal injury or damage to property they might cause).

If you purchase personal goods or services via the Council's Internet service, you are responsible for ensuring that the information you provide shows that the transaction is being entered into by you personally and not on behalf of the Council.

All personal usage must be in accordance with this policy. Your computer and any data held on it are the property of North Lincolnshire Council, this may be accessed at any time by the Council to ensure compliance with all its statutory, regulatory and internal policy requirements.

4.4 Internet Account Management, Security and Monitoring

The Council will provide a secure logon-id and password facility for your Internet account. The Council's IT Services are responsible for the technical management of this account.

All connections to the Internet must be made via a corporate proxy server. The use of external or anonymous proxy servers is prohibited.

You are responsible for the security provided by your Internet account logon-id and password. Only you should know your log-on id and password and you must be the only person who uses your Internet account.

The Council owns the provision of Internet access and all access is recorded, logged and interrogated for the purposes of:

- *Monitoring total usage to ensure business use is not impacted by lack of capacity.*

- *The filtering system monitors and records all access for reports that are produced for line managers, Human Resources and auditors.*

4.5 What you must NOT do

Access to the following categories of websites are currently blocked using a URL filtering system:

- *Adult Material*
- *Social Networking & Personal Sites (see 4.6)*
- *Proxy Avoidance*
- *Hacking*
- *MP3 & Audio Download Services*
- *Illegal or Questionable*
- *Tasteless*
- *Violence*
- *Weapons*
- *Abused Drugs*
- *Militancy & Extremist*
- *Racism & Hate*
- *Web Chat & Instant Messaging*
- *Personal Network & Storage*
- *Peer to Peer File Sharing*
- *Malicious Websites, including spyware, phishing & fraud, key loggers, potentially unwanted software and both networks.*

If a website is currently blocked under one of the above categories and access is required for business use (requires a legitimate business case), it is possible for access to be granted to a user or groups of users. A request should be logged with the IT Servicedesk. The Internal Audit section will review the request and will either deny or allow IT Services to grant access. If you have inadvertently accessed a blocked web site or have been presented with content that you believe should be blocked please contact the IT Servicedesk.

You must **not** use your Internet account to:

- *Create, download, upload, display or access knowingly, sites that contain pornography or other “unsuitable” material that might be deemed illegal, obscene or offensive.*
- *Subscribe to, enter or use peer-to-peer networks or install software that allows sharing of music, video or image files.*
- *Subscribe to, enter or utilise real time chat facilities such as chat rooms, text messenger or pager programs.*
- *Subscribe to, enter or use online gaming*
- *Subscribe to or enter “money making” sites or enter or use “money making” programs.*
- *Run a private business.*
- *Download any software which has not been authorised by IT Services*

It is illegal to create, access, copy, store, transmit or publish any material which falls into the following categories:

- *National Security: instructions on bomb-making, illegal drug production, terrorist activities.*
- *Protection of Minors: inappropriate forms of marketing, displays of violence or pornography involving minors.*
- *Protection of Human Dignity: incitement to racial hatred or racial discrimination, harassment.*
- *Economic Security: fraud: instructions on pirating credit cards.*
- *Information Security: malicious hacking.*
- *Protection of Privacy: unauthorised communication of personal data, electronic harassment.*
- *Protection of Reputation: libel: unlawful comparative advertising.*
- *Intellectual Property: unauthorised distribution of copyrighted works, e.g. software or music.*

It is unacceptable to create, access, copy, store, transmit or publish any material which:

- *Is obscene or pornographic as defined by the Internet Watch Foundation.*
- *Is subversive to the purposes of the Council.*
- *Is likely to corrupt others.*
- *For the purposes of these Guidelines, obscene and pornographic are defined as follows:*
- *Obscene – indecent, lewd, repulsive.*
- *Pornographic – perverted, indecent.*

When assessing whether material is unacceptable, each case will be judged on its merits, taking into account the individual circumstances.

It is unacceptable to undertake any activity, which is intended to:

- *Corrupt any information held or transmitted on the Internet.*
- *Detect weaknesses in any security infrastructure (testing firewalls, cracking passwords).*
- *Disrupt the normal functioning of the Internet or related services (overloading transactions, introducing viruses, denial of service).*

Access to non-work related on-demand or live streaming media is prohibited. Streaming media technologies include, but are not limited to; chat rooms, web casts, video, voice over IP, videoconferencing, web TV, Internet radio.

Websites that stream media content include, but are not limited to; myspace, google videos, skype.

The above list gives examples of "*unsuitable*" usage but is neither exclusive nor exhaustive. *"Unsuitable"* material would include data, images, audio files or video files the transmission of which is illegal under British law, and, material that is against the rules, essence and spirit of this and other Council policies.

4.6 Social Media Sites

Social media is a term used to refer to online technologies and practices that are used to share opinions and information, promote discussion and build relationships. It is equally useful for use by communications staff and policy makers.

Social media services and tools involve a combination of technology, telecommunications and some kind of social interaction. They can use a variety of different formats, for example text, pictures, video and audio.

The term 'social media' is applied to the tools in question, their applications and collaboratively developed practices. Social media applications include, but are not limited to:

- Blogs, for example Blogger
- Online discussion forums, such as Ning, Communities of Practice
- Collaborative spaces, such as Wetpaint
- Media content sharing services, for example YouTube and Flickr
- Micro-blogging applications, for example Twitter
- Social networking sites, such as Facebook, MySpace and Bebo
- Social bookmarking websites, for example Delicious

Access to the use of social networking sites and micro-blogging applications are restricted. However, in some cases access has been permitted to individuals. For example, work on the council's website, e-communications, online-marketing and engagement activities.

Where there is a specific business need to use social networking sites and micro-blogging applications, requests need to be made to the Head of IT Services. These requests will be reviewed in consultation with the Digital Development Group and/or Audit where appropriate.

All council representatives should bear in mind that information they share through social media applications, even if they are on private spaces, are still subject to copyright, data protection and Freedom of Information legislation, the Safeguarding Vulnerable Groups Act 2006 and other legislation. They must also operate in line with the council's Equality scheme and Diversity Policy.

To help with using social media you must adhere to the council's social media guidance. Users accessing such applications must also adhere to the following:

- *Users must not use personal logon accounts*

- *Users must create a business account that clearly states that its ownership and use belongs to North Lincolnshire Council*

- *Business accounts belonging to North Lincolnshire Council must not be used for personal reasons*

- *Access to the account should also be shared by the line manager for mediation*

- *Information published using this technology must not risk placing North Lincolnshire Council into disrepute or disclose any confidential information*

4.7 Your Responsibilities

It is your responsibility to:

- *Familiarise yourself with the detail, essence and spirit of this policy before using the Internet facility provided for your work.*

- *Assess any risks associated with Internet usage and ensure that the Internet is the most appropriate mechanism to use.*

- *Know that you may only use the Council's Internet facility within the terms described herein.*

- *Read and abide by the following related policies:*

    - Email Acceptable Use Policy
    - Technical Strategy
    - Information Security Policy
    - Home Working Policy
    - Employee code of conduct

- *When working with Children Workers must:*

    - Ensure communication takes place within clear and explicit professional boundaries, this includes the wider use of technology such as mobile phones text messaging, e-mails, digital cameras, videos, web-cams, websites and blogs.
    - Not share any personal information with a child;
    - Not request, or respond to, any personal information from a child, other than that which may be appropriate as part of their professional role;
    - Not give their personal contact details to children, including their mobile number, home phone or personal e-mail address, unless the need to do so is agreed with senior management and parents;
    - Only use equipment e.g. mobile phones, provided by their organisation to communicate with children, making sure that parents/carers have given permission for this form of communication to be used;
    - Only make contact with children for professional reasons and in accordance with organisational policy;
    - Only use text messaging as a last resort when no other forms of communication are possible;
    - Not use internet or web-based communication channels to send messages;
    - Use internal e-mail systems in accordance with the organisation's policy.

4.8 Line Manager's Responsibilities

It is the responsibility of Line Managers to ensure that the use of the Internet facility:

- *Within an employee's work time is relevant to and appropriate to the Council's business and within the context of the users responsibilities.*

- *That any new starter is made aware that such policy exists.*

- *Within employee's own time is subject to the rules contained within this document.*

- *Where Social Networking Sites are used to contact children, regular mediation and monitoring should take place.*

4.9 Who Should I Ask if I Have Any Questions?

If you have any questions or comments on the Internet Acceptable Use Policy, please contact the IT Servicedesk, Ext 5555 or 01724 296288. Alternatively, email; servicedesk@northlincs.gov.uk . A call reference number will be issued.

If you do not have any questions, North Lincolnshire Council presumes that you understand and are aware of the rules and guidelines within this policy and will adhere to them

4.10 Acceptable Use

Each user must read, understand and sign to verify they have read and accepted this policy. The Council will be using a system called Policy Matters to manage this process.

4.11 Reporting suspected abuse

If you suspect another individual has misused the Internet or is abusing the use of the Internet, please report this to your line manager in the first instance before involving internal audit.

5. Policy Compliance

5.1 If any individual is found to have breached this policy, they will be subject to North Lincolnshire Council 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.

6. Policy Governance

6.1 The following table identifies who within North Lincolnshire 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	Head of IT Services
Accountable	[Insert appropriate Job Title – e.g. Section 151 Officer, Director of Finance etc. It is important that only one role is held accountable.]
Consulted	IT Strategy Group, Internal Audit, Human resources, Corporate Consultancy Group
Informed	All Council Employees, All Temporary Staff, Members, All Contractors.

7. Review and Revision

7.1 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 Head of IT Services.

8. Definition of Terms

Internet
A computer network consisting of a worldwide network of computer networks that use the TCP/IP network protocols to facilitate data transmission.

Smart phone Device
A Smart phone is a mobile phone offering advanced capabilities beyond a typical mobile phone, often with PC-like functionality.

LADO
Local Authority Designated Officer

Proxy Server
In computer networks, a proxy server is a server (a computer system or an application program) that acts as a go-between for requests from clients seeking resources such as web pages from other servers

Peer-to-Peer
A system in which two or more nodes or processes can initiate communications with each other. Usually describes a network in which all nodes have the ability to share resources with other nodes so that a dedicated server can be implemented but is not required.

SNS Social Network Sites.
A social network service focuses on building online communities of people who share interests and/or activities, or who are interested in exploring the interests and activities of others. Most social network services are web based and provide a variety of ways for users to interact, such as e-mail and instant messaging services.

Email Acceptable Use Policy

NORTH LINCOLNSHIRE COUNCIL

IT Services

Asset Management and Culture

Email Acceptable Use Policy

CONTENTS

Page

1. Purpose of the Policy

1.1 The purpose of the Email Acceptable Use Policy is to ensure appropriate use of the North Lincolnshire Council's email system and to make its users aware of what North Lincolnshire Council deems to be acceptable and unacceptable.

North Lincolnshire Council reserves the right to amend this policy at its discretion. In case of amendments, email users will be informed appropriately. The policy does not grant the employee any contractual rights.

2. Email risks

2.1 The North Lincolnshire Council email system is a business communication tool and its users are obliged to use this tool in a responsible, effective and lawful manner. Although by its nature email seems to be less formal than other written communications, the same laws apply. Therefore, it is important that users are aware of the legal risks of email:

- *If you send or forward emails with any libelous, defamatory, offensive, racist or obscene remarks, you and North Lincolnshire Council can be held liable.*
- *If you unlawfully forward, copy or edit messages without permission, you and North Lincolnshire Council can be held liable for copyright infringement.*
- *If you send an attachment containing a virus, you and North Lincolnshire Council can be held liable*.

2.2 By following the guidelines in this policy, the user can minimise the legal risks involved in the use of email. If any rules set out in this policy are disregarded, the email user will be fully liable and North Lincolnshire Council will disassociate itself from the user as far as legally possible.

3. Legal requirements

3.1 The following rules are required by law and are should be strictly adhered to. It is prohibited to:

- *Send or forward emails containing offensive or disruptive content, which includes, but is not limited to defamatory, offensive, racist or obscene remarks. If you receive an email of this nature, you must promptly notify the IT Servicedesk to record this.*
- *Send unsolicited email messages.*
- *Forge or attempt to forge email messages.*
- *Disguise or attempt to disguise identity when sending mail.*
- *Send email messages using another person's email account.*
- *Copy a message or attachment belonging to another user without the permission of the originator.*

4. Applying the Policy

4.1 Individual responsibility

North Lincolnshire Council considers email as an important means of communication; it recognises the importance of proper mail content, speedy replies in conveying a professional image and delivering good customer service. However, users should take the same care in drafting an email as they would for any other communication. Therefore North Lincolnshire Council expects email users to adhere to the following:

- ***Do not*** *use email as a filing system, use alternative and recognised filing systems available within the Council.*
- *Take extra care in checking that the mail is being sent to the correct person or persons.*
- *Spell check all mail prior to transmission.*
- *When absent from work, (i.e. annual leave) you should enable your 'out of office' message. If a user forgets to set the 'out of office,' a request from the line manager via email to the IT Servicedesk must be made to have this facility enabled. Having the 'out of office' reset also means having the email password reset. A request for a new password must be made by the line manager, via email to the IT Servicedesk upon the users return to work.*
- *Ensure other North Lincolnshire Council email users can view their calendars at all times.*
- ***Do not*** *send unnecessary attachments, use document links.*
- *When 'replying with history', reply 'without attachments' whenever possible.*
- *When 'forwarding with history', forward 'without attachments' if possible.*
- *The use of a North Lincolnshire Council email address for personal purposes is prohibited (i.e. trading, shopping, gaming, gambling sites, etc) If an email user has registered on such a site, this should be unsubscribed/removed with immediate effect. The personal use of a North Lincolnshire Council email address for medical, schooling/child care purposes, etc, is permitted.*
- *Delete any email messages that you do not need a copy of or do not need to retain.*
- *Move emails into folders as they arrive, this increases the overall performance of the mail file.*
- ***Do not*** *use email for distributing information regarding items for sale, public events, and general site specific council news. Information of this nature should be posted on North Lincolnshire Council's Intralinc. The email system may be used to inform colleagues of specific employee news items i.e. colleagues leaving or giving birth.*
- *Changes to email groups, personal name changes, services area changes should be logged with the IT Servicedesk. Failure to notify the IT Servicedesk of changes may result in incorrect email communications being sent.*
- *In the event of a forgotten password, an email request to the IT Servicedesk from your line manager must be made. Passwords cannot be acquired over the phone.*

- *All generic email accounts must be accessed via an individuals email account as part of Government Connect CoCo Compliance.*

- *As a result of Government Connect, automatic forwarding of emails has been removed to non North Lincolnshire Council email addresses.*

- *If you receive any suspicious emails, please leave in your inbox and report immediately to the IT Servicedesk. Never reply to emails requesting information such as, bank account details, PIN Numbers, passwords or personal information.*

- *Never send any confidential, sensitive or personal information (i.e. PIN numbers, bank account information, etc) via the email system. If you are in any doubt whether to send certain information via email, check this with your supervisor/line manager first.*

- *Emails to be sent are restricted to 80Mb in size. Emails greater than 80Mb will be rejected. Emails containing zipped files, which when uncompressed are over 80Mb will also be rejected.*

4.2 General Use of the NLC Email System

It is strictly forbidden to use North Lincolnshire Council's email system for sending 'junk' emails, chain mail, photos, jokes and executable files of a non-business nature. All messages distributed via the email system are North Lincolnshire Council's property.

If you receive spam/suspicious emails, please leave the email in your inbox. Please report the incident to the IT Servicedesk immediately. The email will be investigated, reported and blocked if required. You will then be advised when the email can be deleted.

When an email has been sent in error and a request to delete the email is made, the request must come from their line manager via the IT Servicedesk. This request is then submitted to Internal Audit. Internal Audit will then advise if IT Services can delete the email.

Internal Audit will then advise IT Services, who will advise the line manager of the decision.

Confidential information

Email encryption should be used when emailing confidential or sensitive data. Government Connect Secure Mail can be used to send sensitive, confidential information to other Government agencies or Public Sector organisations. Please contact the IT Servicedesk if you require any of these facilities.

Disclaimer

The following disclaimer will be added to the bottom of each internal and outgoing email message.

This e-mail expresses the opinion of the author and is not necessarily the view of the Council. Please be aware that anything included in an e-mail may have to be disclosed under the Freedom of Information Act and cannot be regarded as confidential. This communication is intended for the addressee(s) only. Please notify the sender if received in error. All email is monitored and recorded. Please think before you print- North Lincolnshire Council greening the workplace.

System monitoring

Users expressly waive any right of privacy in anything they create, store, send or receive on North Lincolnshire Council's email system.

North Lincolnshire Council can, but is not obliged to, monitor emails without prior notification. If there is evidence that you are not adhering to the guidelines set out in this policy, North Lincolnshire Council reserves the right to take disciplinary action, including termination and / or legal action.

All outbound and inbound emails are filtered for inappropriate content, recognised Spam, phishing attacks and certain attachments types. A full list of prohibited attachments can be seen in Section 8 of this Policy. An End User Digest facility providing self-management of quarantined emails is available via the IT Servicedesk. All outbound and inbound emails are filtered for known viruses.

4.3 Email archiving, retention and security

- North Lincolnshire email accounts cannot be forwarded to external addresses. The facility has been removed in accordance with Government Connect Guidelines.
- All emails will be automatically archived to a central secured repository after 90 days based on the current archive/retention policies in place.
- Emails that have been deleted will remain in your 'trash' folder for 48 hours (default period) after this time the 'trash' folder will be cleared automatically.
- Deleted emails can only be restored if, an investigation takes place, FOI requests or at the discretion of your line manager/IT Services.
- Ephemeral emails, read as they arrive, deleted and removed from your trash folder cannot be restored.
- All emails accounts will be backed up overnight and secured offsite.
- When an email user leaves North Lincolnshire Council, their entry in the North Lincolnshire Address Book will be deleted, the mail file for that person will be saved for a period of 90 days. After 90 days the mail will be deleted. Access to the users mailbox or the forwarding of the users mail can only be gained through line manager authorisation
- Email records conveniently fall into one of three categories; statutory, non-statutory and ephemeral and are retained according to their category:
  - ➢ *Statutory records will normally have a retention period included in the appropriate legislation.*
  - ➢ *For Non-Statutory records, the Council has adopted the retention guidelines produced by the Records Management Society of Great Britain and available on the Intralinc.*
  - ➢ *Ephemeral emails are those used purely for immediate information purposes. They can be deleted once read.*

Alternatively please refer to the http://www.rms-gb.org.uk/resources/91 for more information regarding local authority retention policy.

4.4 Email accounts

- All email accounts maintained on the email system are the property of North Lincolnshire Council.
- Passwords should not be given to any other person(s) unless fully authorised to do so. Should you believe there has been a breach of security, please inform the IT Servicedesk.
- Users will be asked to change their passwords every 90 days. Passwords must contain 8 characters or above and contain at least one capital letter and one alphanumeric. Passwords cannot be reused until after the 10th password change. If you forget your password, a request for a password reset must be made by your line manager, via email to the IT Servicedesk. Passwords cannot be given out over the phone.
- Upon leaving your desk area, user information should be cleared to enable password protection whilst you are away from the office. Those using web-based mail should log out of email.
- I-notes (webmail) users will automatically be disconnected after 15 minutes of inactivity.

4.5 Mobile device security and the Email Acceptable Use Policy

The Email Acceptable Use Policy also applies to all users accessing email on a portable/mobile device (i.e. Blackberry users)

The following security will also be applied to the Blackberry device itself in line with Government Connect CoCo compliances:

- Enforced password change to access device every 90 days.
- Passwords must be minimum of 10 characters in length and contain one capital and one alphanumeric.
- Passwords cannot be reused until after the 15th password change.
- All devices will lock after 15 minutes of inactivity. The password will be required to unlock the device.
- Manual changes to passwords are disabled.
- Maximum password attempts are set to ten. If the password is entered incorrectly ten times this will result in the automatic deletion of all device data. The device will be wiped clean and will have to be reconfigured by IT Services.
- All content on the mobile device/Blackberry will be encrypted.
- All content is compressed allowing for more data to be stored on the device.

If you lose or believe your password has been breached, please report this, at the earliest opportunity to the IT Servicedesk on ext. 5555 or 01724 296288. Once notified, the Blackberry will be remotely wiped clean of all its data.

4.6 Email Filtering

Prohibited file attachments

The following is a list of prohibited file attachments. Any email containing one of these will be placed into quarantine:

Ade ,Adp, App, Bas, Bat, Chm, Cmb, Com, Cpl, Dll, Exe, Fxp, Hta, Inf, Ins, Isp, Js, Jse, Ksh, Lib, Lnk, Mdz, Msc, Msi, Msp, Mst, Obj, Ops, Pcd, Pif, Prf, Prg, Reg, Req, Scf, Scr, Sct, Sea, Shb, Shs, Sys, url, vb, vbe, vbs, Wmf, wsc, wsf, wsh, xsl, *wmv, *wma, *mp3, *avi, *mpeg4, *mpe, *mov, *mp4, *mpeg, *fla, *swf, *rm, *ra, *divx, *wav, *asf.

Should you have clear business related reason why you may need to send or receive one of these file types, please contact the IT Servicedesk.

Notification of quarantined emails

The senders of emails containing the following attachment types will receive notification that their email has been quarantined. Contact details are provided should the sender believe the email has been incorrectly quarantined.

Attachment types which produce an automated response are :

*wmv *wma *mp3 *avi *mpeg4 *mpe *mov *mp4, *mpeg *fla *swf *rm *ra *divx *wav *asf *password protected zipped files.

The email received by the sender will appear as follows:

From : Servicedesk@northlincs.gov.uk
To: Sender

Subject: Notification to Sender of Quarantined Email

Text: An email sent to *$OriginalRecipients* on *$CurrentDate $CurrentTime* has been quarantined due to the attachment of prohibited file types which is against the Email Acceptance Use Policy.

For further information on how to send your email using alternative methods please contact the IT Servicedesk on Ext. 5555 or 01724 296288.

Password Protected Emails

Emails sent containing password protected files are automatically quarantined. The email the sender will receive will appear as:

From: Servicedesk@northlincs.gov.uk
To: Sender

Subject: Notification to Sender of Quarantined Email

Text: An email sent to *$OriginalRecipients* on *$CurrentDate $CurrentTime* has been quarantined due to the use of Password Protected files which is against Email Acceptance Use Policy..

For further information on how to send your email using alternative methods please contact the IT Servicedesk on Ext. 5555 or 01724 296288.

4.7 Line Manager's Responsibilities

It is the responsibility of Line Managers to ensure that the use of the Email facility:

- Within an employees work time, is relevant to and appropriate to the Council's business and within the context of the users responsibilities.
- New starters are made aware that such the policy exists.
- Within employees own time is subject to the rules contained within this document.

4.8 Who should I ask if I have any questions?

If you have any questions or comments on the Email Policy, please contact the IT Servicedesk, Ext 5555 or 01724 296288. Alternatively, email; servicedesk@northlincs.gov.uk. These queries will be recorded and responded to by the appropriate officer.

If you do not have any questions North Lincolnshire Council presumes that you understand and are aware of the rules and guidelines in this email policy and will adhere to them.

4.9 Acceptable Use

Each email user must read, understand and sign to verify they have read and accepted this policy. The authority will be using a system called 'Policy Matters' to manage this process.

4.10 Reporting suspected abuse

If you suspect another individual has misused the email system, please report this to your Line Manager before involving internal audit.

5. Policy Compliance

5.1 If an individual is found to have breached this policy, they will be subject to North Lincolnshire Council 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.

6. Review and Revision

6.1 This policy will be reviewed as it is deemed appropriate, but no less frequently than every 12 months. The policy review will be undertaken by the Head of IT Services