North Yorkshire County Council

Policy Document PO 26

Email

04 Sept 2012

Document Control

Organisation	North Yorkshire County Council
Title	Senior Information Security Compliance Officer
Author	ITSO
Filename	NYCC Email Policy.doc
Owner	Senior Information Security Compliance Officer
Subject	Email usage
Protective Marking	Unrestricted
Review date	Sept 2013

Revision History

Revision Date	Revisor	Previous Version	Description of Revision
14 Sept 09	ITSO	V1.1	Sects 8 insert responsibility Chief Information Officer. Insert consulted Data Management Officer. Section 3 third paragraph remove in entirety Section 6.8 para 3 remove unclassified, confidential, Secret and Top Secret
17 Sept 09	ITSO	V1.2	Insertion of section 6.3 email signature directive
14 Oct 09	ITSO	V1.3	Sect 6.6 para 3 line 5 delete 50mb insert 10mb
10 May 10	ITSO	V1.4	Remove all instances of Harassment, discrimination and bullying policy and replace with Resolving issues at work policy.
08 Jul 10	ITSO	V1.5	Sects 6.2 para 9 insert outgoing important emails. Sect 6.2 para 9 remove make and keep copies insert store copies. Amend review date to Jul 2010 Sect 6.1 para 2 delete 6.7 insert 6.8. 6.2 para 5 bullet 23 in insert This may be by use of group email address or by being granted proxy access to another person's mailbox. Change to header remove word Internal. Remove word policy from title
15 Sept 10	ITSO	V1.6	Sub section 6.31 scanned signatures added
02 Nov 10	ITSO	V1.7	Sect 7 insert Officers of the County Council are required to comply with this policy in respect of its provisions and ethos. Failure to do so may be regarded as a breach of the Officers' Code of Conduct and could result in action being taken against the member of staff concerned.
27 Sept 11	ITSO	V1.8	Sect 3 insert This policy applies to, but is not, limited to NYCC councillors, employees (including casual, agency workers, secondees, contractors and contractual third parties) who have access to the Council's Internet service and/or ICT equipment.
02 May 12	SISCO	V1.9	Review due to PWC audit. Remove all instances of groupwise and change to Outlook. Section 6.6 para 2 change mailbox size from 500mb to 1Gb.
04 Sep 12	SISCO	V2.0	Insertion of section 6.12 messenger services

Document Approvals

This document requires the following approvals:

Sponsor Approval	Name	Date
Senior Information Risk Officer		
Corporate Information Governance Group		13 09 2012

Contributors

Development of this policy was assisted through information provided by the following organisations:

Contents

1 Policy Statement

North Yorkshire County Council will ensure all users of Council email facilities are aware of the acceptable use of such facilities. The County Council has a legal responsibility with regard to acceptable use of email within the County Council. The County Council must comply with the following legal statutes:

- Sexual Offences Act
- EU Privacy and Monitoring Directive
- Regulation of Investigatory Powers Act
- Human Rights Act
- Freedom of Information Act
- Data Protection Act
- Computer Misuse Act
- Copyright, Design and Patents Act

2 Purpose

The objective of this Policy is to direct all users of Council email facilities by:

- Providing guidance on expected working practice.
- Highlighting issues affecting the use of email.
- Informing users about the acceptable use of ICT facilities in relation to emails.
- Describing the standards that users must maintain.
- Stating the actions that may be taken to monitor the effectiveness of this policy.
- Warning users about the consequences of inappropriate use of the email service.

The Policy establishes a framework within which users of Council email facilities can apply self-regulation to their use of email as a communication and recording tool.

3 Scope

This policy covers all email systems and facilities that are provided by North Yorkshire County Council for the purpose of conducting and supporting official business activity through the Councils network infrastructure and all stand alone and portable computer devices.

This policy applies to, but is not, limited to NYCC councillors, employees (including casual, agency workers, secondees, contractors and contractual third parties) who have access to the Council's Internet service and/or ICT equipment.

The policy also applies where appropriate to the internal Microsoft Exchange (Outlook), Webmail and Live Remote e-mail facilities which may be accessed by many staff who are not authorised Internet and e-mail users.

The use of email facilities by staff that have not been authorised for that purpose will be regarded as a disciplinary offence.

Please refer to the ICT Access Policy for information on how to request a corporate or GCSX email account.

4 Definition

All email prepared and sent from North Yorkshire County Council email addresses or mailboxes, and any non-work email sent using North Yorkshire County Council ICT facilities is subject to this policy.

Glossary of Definitions

Electronic mail (abbreviated "e-mail" or, often, "email") is a store and forward method of composing, sending, storing, and receiving messages over electronic communication systems.

An **email client** is a computer programme that is used to read and send email.

Email **spam** involves sending nearly identical unauthorised, unsolicited messages to numerous recipients by email.

A **record** is information created, received and maintained as evidence and information by an organisation or person, in pursuance of legal obligations, or in the transaction of business (BS ISO 15489-1).

5 Risks

North Yorkshire County 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:

- Loss of data or information and data protection issues
- Misuse of the corporate email system
- Legal issues

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**.**

6 Applying the Policy

6.1 Email as Records

All emails that are used to conduct or support official North Yorkshire County Council business must be sent using an authorised email address for example “@northyorks.gov.uk” “@veritau.co.uk. All emails sent via the Government Connect Secure Extranet (GCSx) must be of the format “@northyorks.gcsx.gov.uk”.

Non-work email accounts **must not** be used to conduct or support official North Yorkshire County Council business. Councillors and users must ensure that any emails containing sensitive information must be sent from an official council email. Any emails containing RESTRICTED information being sent to another Public Sector organisation must be sent from a GCSx email. (Please also refer to section 6.8). All emails that represent aspects of Council business or Council administrative arrangements are the property of the Council and not of any individual employee.

Emails held on Council equipment are considered to be part of the corporate record and email also provides a record of staff activities.

The legal status of an email message is similar to any other form of written communication. Consequently, any e-mail message sent from a facility provided to conduct or support official North Yorkshire County Council business should be considered to be an official communication from the Council. In order to ensure that North Yorkshire County Council is protected adequately from misuse of e-mail, the following control will be exercised:

i. All official external e-mail must carry the following disclaimer:

"Access your county council services online 24 hours a day, 7 days a week at www.northyorks.gov.uk.

WARNING

Any opinions or statements expressed in this e-mail are those of the individual and not necessarily those of North Yorkshire County Council.

This e-mail and any files transmitted with it are confidential and solely for the use of the intended recipient. If you receive this in error, please do not disclose any information to anyone, notify the sender at the above address and then destroy all copies.

North Yorkshire County Council's computer systems and communications may be monitored to ensure effective operation of the system and for other lawful purposes. All GCSX traffic may be subject to recording and/or monitoring in accordance with relevant legislation.

Although we have endeavoured to ensure that this e-mail and any attachments are free from any virus we would advise you to take any necessary steps to ensure that they are actually virus free.

If you receive an automatic response stating that the recipient is away from the office and you wish to request Information under either the Freedom of Information Act, the Data Protection Act or the Environmental Information Regulations please forward your request by e-mail to the Data Management Team (datamanagement.officer@northyorks.gov.uk)who will process your request.

North Yorkshire County Council."

Whilst respecting the privacy of authorised users, North Yorkshire County Council maintains its legal right, in accordance with the Regulation of Investigatory Powers Act 2000, to monitor and audit the use of email by authorised users to ensure adherence to this Policy. Any such interception or monitoring will be carried out in accordance with the provisions of that Users should be aware that deletion of e-mail from individual accounts does not necessarily result in permanent deletion from the Council's ICT systems.

It should also be noted that email and attachments may need to be disclosed under the Data Protection Act 1998 or the Freedom of Information Act 2000. Further information regarding this can be obtained from the Data Management Officer.

Officers should also consider, before sending an email, how they would feel if the message was read out in Court. Email messages may have to be disclosed in litigation.

6.2 Email as a Form of Communication

Email is designed to be an open and transparent method of communicating. However, it cannot be guaranteed that the message will be received or read, nor that the content will be understood in the way that the sender of the email intended. It is therefore the responsibility of the person sending an email to decide whether email is the most appropriate method for conveying time critical or PROTECT or RESTRICTED information or of communicating in the particular circumstances.

All emails sent to conduct or support official North Yorkshire County Council business must comply with corporate communications standards. These are available on the intranet
Councillors must ensure that any emails containing sensitive information must be sent from an official council email.

Email must not be considered to be any less formal than memo's or letters that are sent out from a particular service or the authority. When sending external email, care should be taken not to contain any material which would reflect poorly on the Council's reputation or its relationship with customers, clients or business partners.

Under no circumstances should users communicate material (either internally or externally), which is, for example, defamatory, obscene, or does not comply with the Council's Equal Opportunities

Policy, or which could reasonably be anticipated to be considered inappropriate. Any user, who is unclear about the appropriateness of any material, should consult their line manager prior to commencing any associated activity or process.

ICT facilities provided by the Council for email should not be used:

- For the transmission of unsolicited commercial or advertising material, chain letters, or other junk-mail of any kind, to other organisations.
- For any form of illegal activity which will lead to criminal and disciplinary action.
- For the transmission or creation of illegal material.
- For the unauthorised transmission to a third party of PROTECT or RESTRICTED material concerning the activities of the Council.
- To impersonate any other person or amend messages received.
- In the pursuit of private business.
- For the transmission of material such that this infringes the copyright of another person, including intellectual property rights.
- For activities that unreasonably waste staff effort or use networked resources, or activities that unreasonably serve to deny the service to other users.
- For activities that corrupt or destroy other users' data.
- For activities that disrupt the work of other users.
- For the creation or transmission of any offensive, obscene or indecent images, data, or other material, or any data capable of being resolved into obscene or indecent images or material.
- For the creation or transmission of material which is designed or likely to cause annoyance, inconvenience or needless anxiety.
- For the creation or transmission of material that is abusive or threatening to others, or serves to harass or bully others.
- For the creation or transmission of material containing derogatory, insulting or aggressive remarks.
- For the creation or transmission of material that either discriminates or encourages discrimination on racial or ethnic grounds, or on grounds of gender, sexual orientation, marital status, disability, political or religious beliefs.
- For the creation or transmission of defamatory material.
- For the creation or transmission of material that includes false claims of a deceptive nature.
- For so-called 'flaming' - i.e. the use of impolite terms or language, including offensive or condescending terms.
- For activities that violate the privacy of other users.
- For unfairly criticising individuals, including copy distribution to other individuals.
- For publishing to others the text of messages written on a one-to-one basis, without the prior express consent of the author.
- For the creation or transmission of anonymous messages - i.e. without clear identification of the sender. This may be by use of group email address or by being granted proxy access to another persons mailbox
- For the creation or transmission of material which brings the Council into disrepute.
- To enter into contracts.

When using ICT facilities provided by the Council for email Officers should:

- Seek confirmation of receipt of outgoing important emails.
- Store copies of important emails sent and received.
- Include the senders' name, job title and Service Unit.
- Always check the email content can not be misconstrued in anyway before sending it.

It is forbidden to use another person's account/password/userid.

6.2.1 Definitions

1. Illegal Material

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

1. National Security such as instructions on bomb making, illegal drug production or terrorist activities.
2. Abuse in the form of marketing, violence or pornography
3. Incitement to racial hatred or discrimination
4. Economic fraud such as instructions on pirating credit cards
5. How to breach security via malicious hacking

In addition it is necessary to protect the reputation of the authority, by not distributing unauthorised works protected by copyright such as software or music.

2. Forbidden material

For the purposes of this Policy Statement, obscene and vulgar are defined as follows:-

1. Obscene - indecent, lewd, repulsive
2. Vulgar - offending against good taste, coarse

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

Pornography can take many forms. For example, textual descriptions, still and moving images, cartoons, and sound files. Some pornography is illegal in the UK and some is legal. Pornography considered legal in the UK may be illegal elsewhere. Because of the global nature of the Internet and email, these issues must be taken into consideration. Therefore, the County Council defines pornography as the description or depiction of sexual acts or naked people that are designed to be sexually exciting. The County Council will not tolerate its facilities being used for this type of material and considers such behaviour to constitute a serious disciplinary offence

3. Harassment

What is harassment?

The contents of an email can give rise to complaints of harassment. Harassment is a complex and sensitive issue and it can be described as unwanted, unsolicited and inappropriate words or conduct affecting the dignity of another person. It can be isolated or repetitive behaviour and may be directed at an individual or group.

Harassment can also be of a sexual nature. For example:

- Where a worker is subject to any form of unwanted verbal, non-verbal or physical conduct of a sexual nature which has the purpose or effect of violating that worker's dignity or creating an intimidating, hosting, degrading, humiliating or offensive environment for that person;
- It will also take place where the unwanted verbal, non verbal or physical conduct of a sexual nature relate to a person's sex, to the sex of another person, sexual orientation or to the fact that a person intends to undergo or is undergoing or has undergone gender reassignment.

Harassment is considered to be very personal, because what constitutes acceptable behaviour by one individual may be deemed to be harassment by another.

What are the consequences of not following this policy?

In accordance with the information given in the County Council's Policy and Procedure on Resolving issues at work an investigation would be carried out. Many complaints can be resolved through conciliation, but if necessary disciplinary action will be taken against the harasser or bully.

If you are subject to e-mail harassment, keep a copy of all relevant emails. A number of contact officers are available throughout the County Council; the HR Services team can supply the name of an appropriate person to contact. A full copy of the Council's policy on Resolving issues at work is available on the intranet or by contacting the HR Services team.

4. Defamation

What is defamation?

Defamation is the issuance of a statement which exposes a person to hatred, ridicule or contempt or which causes them to be shunned or avoided, or which has a tendency to injure him in his office, profession or trade. If such a statement is published in a form to which some degree of permanence attaches the individual can bring a libel action.

What are the consequences of not following this policy?

The County Council and the sender may risk court action if the County Council's email system is used to disseminate defamatory information.

Any person sending such an email will, if necessary, be disciplined under the County Council's Disciplinary Procedure.

5. Entering Contracts

A contract is an agreement enforceable at law. Employees may inadvertently enter into contracts or vary terms which the County Council would not like to honour.

Officers must not enter into a contract or vary a term of a contract by using the County Council's email system unless it is authorised by an Assistant Director or higher and is in accordance with the Contract Procedure Rules and/or Procurement Guidelines. A breach of this rule could result in the County Council's Disciplinary Procedure being invoked.

6. Personal Data

Personal data is subject to the Data Protection Act 1998. Under the terms of the Act, personal data includes any information about a living individual, including their name, address, phone number Email address and any other information about the individual. If such information is included in an Email or an attachment to an Email, individuals will be deemed to be "processing" personal data and must abide by the law. In particular, they must not collect such information without the person concerned knowing they propose to do this. Such information may not be disclosed or amended except in accordance with the purpose for which the information was collected. Officers must ensure that the information is accurate and up to date. In addition, the individual has the right to inspect what is held about him or her on the Email system. The individual can demand correction of inaccurate information, can request blocking or erasure of damaging information, and can sue for damage caused by in accurate information.

Employees must be aware that although the Data Protection Act states that personal data relates to living individuals, information relating to a deceased person can also constitute personal data therefore it must be handled in the same way as data relating to a ;living individual.

The law imposes rules on the storing of personal data. Such data should be kept only for as long as it is needed for the purpose for which it was collected.

6.3 Email Signature

All staff should follow this email signature format to comply with corporate branding and readability guidelines, and to reduce unnecessary load on email servers.

For many users, the default display for emails is text-only. This means that images and graphics will not be displayed. Therefore, you should not include graphics (including the North Yorkshire County Council logo) in your email signatures.

The standardised email signature, below, provides a consistent brand across the council and ensures signatures can be viewed by all with, or without, rich text editors.

The North Yorkshire County Council standard email signature should appear as follows:

Name: **Bold, Black, Arial, 10pt. font;**
Job title: regular, black, Arial, 10pt. font;
Postal address;
<space>
Telephone number (including STD code) and extension;
Fax number (optional);
Email address: all lower case;
Website address;
<space>

For example:

Joe Bloggs
Communications assistant
North Yorkshire County Council
Communications Unit
County Hall
Northallerton
DL7 8AD

Telephone: 01609 53 6666 | x6666
Email: joe.bloggs@northyorks.gov.uk
www.northyorks.gov.uk

The Disclaimer text will appear below this signature

6.31 Scanned Signature

What is a scanned signature?

A written signature, which has been scanned, that can be embedded into an electronic document.

Using Scanned Signatures

It should be noted that a scanned signature is as valid as a hand written signature, where it is the intention of the signatory to endorse the document.

Efficiencies can be gained by the use of scanned signatures when either sending large volumes of similar correspondence, or to expedite internal approval or communication processes.

With any signature there is a risk that someone may fraudulently use it elsewhere, and the risks are the same whether the signature is on paper, or electronically embedded.

It is a fact that if people wish to misuse signatures, whether they are written or electronic, they will. But we can take some precautions to lessen the inherent security issues resulting from the use of

scanned signatures and to minimise the potential risks of misappropriation and/or inappropriate use of scanned signatures

- No electronic signature may be used without authorisation which must be in writing and signed otherwise than electronic signature from the signatory
- No electronic signature shall be used except for the purpose for which it was authorised, and in accordance with the terms and conditions of the authorisation.
- Steps should be taken to ensure that no one has access to a scanned signature other than those permitted to use it. Generally, documents should be saved without the signature. Where it is necessary to save a signature in a document, it **must** be protected.
- If a document is to be sent by e-mail, or uploaded to the internet/intranet, the signature should be suitably protected.

6.4 Personal Use

Occasional and reasonable personal use of the ICT facilities provided by the Council for email is permitted provided that such use takes place during unpaid hours and it is in adherence with this policy.

Officer sending a personal email should:

1. Include the word 'personal' in the subject field.
2. Start or sign off the email with the following statement:

"This email is personal. It is not authorised by or sent on behalf of North Yorkshire County Council, however, the Council has the right and does inspect emails sent from and to its computer system. This email is the sole responsibility of the sender."

6.5 Junk Mail

There may be instances where a user will receive unsolicited mass junk email or spam. It is advised that users delete such messages without reading them. Do not reply to the email. Even to attempt to remove the email address from the distribution list can confirm the existence of an address following a speculative e-mail.

Before giving your e-mail address to a third party, for instance a website, consider carefully the possible consequences of that address being passed (possibly sold on) to an unknown third party, and whether the benefits outweigh the potential problems.

Chain letter e-mails (those that request you forward the message to one or more additional recipients who are unknown to the original sender) **must not** be forwarded using North Yorkshire County Council systems or facilities.

6.6 Mail Box Size

In order to ensure that the systems enabling email are available and perform to their optimum, users should endeavour to avoid sending unnecessary messages. In particular, the use of the "global list" of e-mail addressees is discouraged.

Users are provided with a limited mail box size 1Gb to reduce problems associated with server capacity. Email users should manage their email accounts to remain within the limit, ensuring that items are filed or deleted as appropriate to avoid any deterioration in systems.

Email messages can be used to carry other files or messages either embedded in the message or attached to the message. If it is necessary to provide a file to another person, then a reference to where the file exists should be sent rather than a copy of the file. This is to avoid excessive use of

the system and avoids filling to capacity another person's mailbox. If a copy of a file must be sent then it should not exceed 10mb in size.

6.7 Monitoring of Email Usage

All users should be aware that email usage is monitored and recorded centrally. The monitoring of email (outgoing and incoming) traffic will be undertaken so that North Yorkshire County Council:

- Can plan and manage its resources effectively.
- Ensures that users act only in accordance with policies and procedures.
- Ensures that standards are maintained.
- Can prevent and detect any crime.
- Can investigate any unauthorised use.

Monitoring of content will only be undertaken by staff specifically authorised for that purpose. These arrangements will be applied to all users and may include checking the contents of email messages for the purpose of:

- Establishing the existence of facts relevant to the business, client, supplier and related matters.
- Ascertaining or demonstrating standards which ought to be achieved by those using the facilities.
- Preventing or detecting crime.
- Investigating or detecting unauthorised use of email facilities.
- Ensuring effective operation of email facilities.
- Determining if communications are relevant to the business.

Where a manager suspects that the email facilities are being abused by a user, they should contact the ICT Senior Information Security Compliance Officer. Designated staff in ICT Services and Internal Audit can investigate and provide evidence and audit trails of access to systems. Internal Audit will also comply with any legitimate requests from authorised bodies under the Regulation of Investigatory Powers legislation for this information.

Access to another employee's email is strictly forbidden unless the employee has given their consent, or their email needs to be accessed by their line manager for specific work purposes whilst they are absent. If this is the case a request can be made via the ICT Service Desk. This must be absolutely necessary and has to be carried out with regard to the rights and freedoms of the employee. Managers must only open emails which are relevant.

6.8 Categorisation of Messages

When creating an email, the information contained within it must be assessed and classified by the owner according to the content, when appropriate. It is advisable that all emails are protectively marked in accordance with the HMG Security Policy Framework (SPF). The marking classification will determine how the email, and the information contained within it, should be protected and who should be allowed access to it.

The SPF requires information to be protectively marked. The way the document is handled, published, moved and stored will be dependant on this scheme.

The classifications are:

- PROTECT.
- RESTRICTED.

Information up to RESTRICTED sent via GCSx must be marked appropriately using the SPF guidance.

6.9 Security

Emails sent between northyorks.gov.uk address are held with the same network and are deemed to be secure. However, emails that are sent outside this closed network travel over the public communications network and are liable to interception or loss. There is a risk that copies of the email are left within the public communications system. Therefore, PROTECT and RESTRICTED material must not be sent via email outside a closed network, unless via the GCSx email, PGP mail or SFTP.

Where GCSx email is available to connect the sender and receiver of the email message, this **must be used** for all external email communicating RESTRICTED material.

All Council employees that require access to GCSx email must read understand and sign the GCSx Acceptable Usage Policy and Personal Commitment Statement.

6.10 Confidentiality

All staff are under a general requirement to maintain the confidentiality of information. There are also particular responsibilities under Data Protection legislation to maintain the confidentiality of personal data. If any member of staff is unsure of whether they should pass on information, they should consult the Data Management Officer.

Staff must make every effort to ensure that the confidentiality of email is appropriately maintained. Staff should be aware that a message is not deleted from the system until all recipients of the message and of any forwarded or attached copies have deleted their copies. Moreover, confidentiality cannot be assured when messages are sent over outside networks, such as the Internet, because of the insecure nature of most such networks and the number of people to whom the messages can be freely circulated without the knowledge of North Yorkshire County Council.

Care should be taken when addressing all emails, but particularly where they include PROTECT or RESTRICTED information, to prevent accidental transmission to unintended recipients. Particular care should be taken if the email client software auto-completes an email address as the user begins typing a name.

Automatic forwarding of email is prohibited. Rules can be implemented to include or exclude certain mail based on the sender or subject. If you require assistance with this, please contact the ICT Service Desk in the first instance.

The automatic forwarding of a GCSx email to a lower classification email address (i.e. a standard .gov.uk email) contradicts national guidelines and is therefore not allowed.

6.11 Negligent Virus Transmission

Computer viruses are easily transmitted via email and internet downloads. Full use must therefore be made of North Yorkshire County Council's anti-virus software. If any user has concerns about possible virus transmission, they must report the concern to the ICT Service Desk.

In particular, users:

- Must not transmit by email any file attachments which they know to be infected with a virus.
- Must not download data or programs of any nature from unknown sources.
- Must ensure that an effective anti-virus system is operating on any computer which they use to access Council facilities.
- Must not forward virus warnings other than to the ICT Service Desk.
- Must report any suspected files to the ICT Service Desk.

In addition, the Council will ensure that email is virus checked at the network boundary and at the host, and uses two functionally independent virus checkers.

If a computer virus is transmitted to another organisation, the Council could be held liable if there has been negligence in allowing the virus to be transmitted. Users must therefore comply with the Software Policy.

6.12 Windows Messenger

Instant messaging is a tool like e-mail that allows a form of text-based communication from one person to another. It operates on a real-time basis, meaning that as long as the required parties are connected to the corporate network and logged in, each party is able to see the connection status of the other and communicate with them almost instantly. Like a phone conversation, Messenger allows users to chat back and forth in real time.

The County Council supports the installation and usage of Windows Messenger as the approved messenger client.

All policies and guidelines pertaining to e-mail content also apply to Messenger, including but not limited to sections regarding solicitation, obscenity, harassment, pornography, sensitive information, bullying and malware.

Messenger can be used for both work related and limited personal use

Messenger Security

Instant messaging, like any other type of software that utilizes network connectivity, has the potential for security-related issues. Messenger communications are sent in clear text, which is not encrypted.

It must be understood that sensitive data that is passed via Messenger could possibly be read by parties other than the intended recipients. Clear text traffic also makes Messenger vulnerable to man-in-the-middle attacks where a malicious third party intercepts and possibly manipulates Messenger traffic. Transferring sensitive data over Messenger is prohibited.

Messenger will not be configured to function as a peer to peer file sharing service.

Usernames will replicate those used for network authentication

The corporate messenger service will be monitored through sampling undertaken by authorised personnel.

7 Policy Compliance

Officers of the County Council are required to comply with this policy in respect of its provisions and ethos. Failure to do so may be regarded as a breach of the Officers' Code of Conduct and could result in action being taken against the member of staff concerned.

If you do not understand the implications of this policy or how it may apply to you, seek advice from the Data Management Officer or the ICT Senior Information Security Compliance Officer. .

8 Policy Governance

The following table identifies who within North Yorkshire County 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	ICT Senior Information Security Compliance Officer.

Consulted	Data Management Officer
Informed	All Council Employees, All Temporary Staff, All Contractors.

9 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 ICT Senior Information Security Compliance Officer.

10 References

The following North Yorkshire County Council policy documents are directly relevant to this policy, and are referenced within this document:

- GCSx Acceptable Usage Policy and Personal Commitment Statement.
- Software Policy.
- ICT Access Policy.

The following North Yorkshire County Council policy documents are indirectly relevant to this policy:

- Internet Usage Policy.
- Computer, Telephone and Desk Use Policy.
- Remote Working Policy.
- Removable Media Policy.
- Information Security Incident Management Policy.
- Employee Guide to Information Security
- Data Protection Policy
- Freedom of Information Policy

11 Key Messages

- All emails that are used to conduct or support official North Yorkshire County Council business must be sent using a "@northyorks.gov.uk" address.
- All emails sent via the Government Connect Secure Extranet (GCSx) must be of the format "@northyorks.gcsx.gov.uk".
- Non-work email accounts **must not** be used to conduct or support official North Yorkshire County Council business.
- Councillors and users must ensure that any emails containing sensitive information must be sent from an official council email.
- All official external e-mail must carry the official Council disclaimer (see section 6.1).
- Under no circumstances should users communicate material (either internally or externally), which is defamatory, obscene, or does not comply with the Council's Equal Opportunities policy.
- Where GCSx email is available to connect the sender and receiver of the email message, this **must be used** for all external email use and must be used for communicating PROTECT and RESTRICTED material.
- Automatic forwarding of email must be considered carefully to prevent PROTECT and RESTRICTED material being forwarded inappropriately.

North Yorkshire County Council

Policy Document PO 28

Internet Usage Policy

02 May 2012

Document Control

Organisation	North Yorkshire County Council
Title	Internet Acceptable Usage Policy
Author	C Wright
Filename	NYCC Internet Acceptable Usage Policy
Owner	ICT Information Security Officer
Subject	Internet Policy
Protective Marking	Unrestricted
Review date	May 2013

Revision History

Revision Date	Revisor	Previous Version	Description of Revision
07/07 2010	ITSO	1.3	Rename policy Internet usage policy, remove wording acceptable. Change review date and version number. Remove section 6.9 acceptable statement and signature. Section 8, Governance delete Chief Information officer insert Senior Information Risk Officer, Delete Data officer insert Audit and Information Assurance Manager
02/11/10	ITSO	1.4	Insert Officers of the County Council are required to comply with this policy in respect of its provisions and ethos. Failure to do so may be regarded as a breach of the Officers' Code of Conduct and could result in action being taken against the member of staff concerned.
27/09/11	ITSO	1.5	Review of scope statement and amendment to cover including casual, agency workers, secondees, contractors and contractual third parties
15/11/11	ITSO	1.6	Section 5 para 4 change Human Rights Act to Human Rights Act 1998. Insert Data Protection Act 1998 and Telecommunications (Unlawful Business Practice) Interception of Communications Regulations 2000. Sections 6.6 remove ICT Access Policy.
02/05/2012	ITSO	1.7	Review due to PWC Audit

Document Approvals

This document requires the following approvals:

Sponsor Approval	Name	Date
Senior Information Risk Officer		
Assistant Director of ICT Services		24 09 2009
Audit and Information Assurance Manager		23 09 2009

Document Distribution

This document will be distributed to:

Name	Job Title	Email Address

Contributors

Development of this policy was assisted through information provided by the following organisations:

- Devon County Council
- Dudley Metropolitan Borough Council
- Herefordshire County Council
- Plymouth City Council
- Sandwell Metropolitan Borough Council
- Sefton Metropolitan Borough Council
- Staffordshire Connects
- West Midlands Local Government Association
- Worcestershire County Council

Contents

1 Policy Statement

North Yorkshire County Council will ensure all users of Council provided internet facilities are aware of the acceptable use of such facilities. This document explains the policy and procedure that governs use of the *Internet* and *World Wide Web* within the Council. Compliance with this policy will ensure that access to the Internet will be available and responsive to the business needs of the Council.

2 Purpose

This policy document tells you how you should use your Council Internet facility. It outlines your personal responsibilities and informs what you must and must not do.

The Internet facility is made available for the business purposes of the Council. A reasonable 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. Use of the Internet is encouraged in the execution of day-to-day business to the extent that it supports the council's objectives. Users must not use the Internet within the council in the same way they do at home—all users must respect the council's standards of business conduct whenever the Internet is used.

3 Scope

This policy applies to, but is not, limited to NYCC councillors, employees (including casual, agency workers, secondees, contractors and contractual third parties) who have access to the Council's Internet service and/or ICT equipment

4 Definition

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 computer or a Smartphone device.

4.1 DEFINITIONS/GLOSSARY

The *Internet* is a system of computer networks that are located all over the world, linked together to allow computers on these networks to communicate and exchange information. The Internet is not synonymous with the *World Wide Web*

A *web browser* is a software application programme that provides a way to look at and interact with all the information on the *World Wide Web*.

A *website* (web site or simply, site) is a set of interconnected web pages, usually including a homepage, and prepared and maintained as a collection of information by a person, group, or organisation.

The *World Wide Web* (www or simply, the Web) is a way of exchanging information between computers on the *Internet*, tying them together into a vast collection of interactive multimedia resources. The World Wide Web is not synonymous with the *Internet*.

5 Risks

North Yorkshire County 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:

- Inappropriate use of the Internet Facility
- Legal Issues

- Data and Information protection issues

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. The council has a legal responsibility with regard to Internet access control and monitoring. The council must comply with the following legal statutes:

Human Rights Act 1998
Sexual Offences Act 2003
EU Privacy and Monitoring Directive 2000
Regulation of Investigatory Powers Act 2000
Data Protection Act 1998
Telecommunications (Unlawful Business Practice) Interception of Communications Regulations 2000

6 Applying the Policy

6.1 What is the Purpose of Providing the Internet Service?

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

- 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.

6.2 What You Should Use Your Council Internet Access For

Your Council Internet access 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 authorised equipment for the Council).

6.3 Personal Use of the Council's Internet Service

The Council permits limited personal use of the Internet in your own time (for example during your lunch-break), however the internet must not be used for personal use during 'paid hours' and should not

Consume a significant amount of resources, including staff time
Interfere with staff productivity or performance
Involve significant costs to the council
Detrimentally affect the council's business interests, reputation, or cause loss of goodwill to the council
Business use of the Internet takes precedence over personal use at all times

The Council is not, however, responsible for any personal transactions you enter into - for example 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 - for example in relation to payment 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.

You should ensure that personal goods and services purchased are not delivered to Council property. Rather, they should be delivered to your home or other personal address.
If you are in any doubt about how you may make personal use of the Council's Internet Service you are advised not to do so. Further information is available from ICT Services.

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

6.4 Internet Account Management, Security and Monitoring

Access to the Internet is granted by your Director who will authorise employees to use the Internet where it is an integral part of their duties and responsibilities. There are different levels of access to the Internet, the majority of staff will be given default access, bands 0-2. Please refer to Appendix 1 for details of the Council's Internet Access Bands.

Additional access can be requested by completing an Internet Access Form and submitting it via your ICT Client team to the ICT Service Desk. A copy of the Internet Access Form is available on the intranet. The Directors will annually review the employees with Internet Access higher than default to make sure it is still appropriate for their duties and responsibilities.

Those granted access to the internet do so by logging on to the Council's network with their computer username and password. The Council's ICT Services is responsible for the technical management of this account.

You are responsible for the security provided by your computer account username and password. Only you should know your username and password and you should be the only person who uses your Internet account.

The provision of Internet access is owned by the Council and all access is recorded, logged and interrogated for the purposes of resource management and compliance to current policies and legislation: To help enforce this policy, the council has invested in technology to filter and monitor the usage of its Internet connection. The Internet filtering and monitoring system is used to:

Monitor, analyse, and track all access to the Internet within the council
Categorise websites based on content
Allow or block access to websites by category, keyword, bandwidth, and file type
Reduce legal liability associated with Internet misuse
Produce logs and reports (for example, to list website names and time spent on them by each user, track attempts to visit blocked sites, track usage trends etc and make these available for line managers and auditors

Users who fail to follow this policy risk disciplinary action. The council acknowledges its obligation to report any illegal activities to the appropriate authorities

Access to the Internet via the council's network is only possible using computers issued by the council—assembled using standardised hardware and software and connected to the council's computer network. The *web browser* used by the council is Microsoft Internet Explorer®.

6.5 Things You Must Not Do

Access to the following categories of websites is currently blocked using URL filtering:

- Illegal.
- Pornographic.
- Violence.
- Hate and discrimination.
- Offensive.
- Weapons.
- Hacking.
- Web chat.
- Gambling.
- Dating.
- Radio stations.

- Games.
- Streaming media
- E-Bay
- YouTube
- Social networking sites

However if you have a legitimate business reason to access the above categories you can request access by completing an Internet Access Form (See section 6.4).

Except where it is strictly and necessarily required for your work, for example IT audit activity or other investigation, 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 or betting sites.
- Subscribe to or enter "money making" sites or enter or use "money making" programs.
- Subscribe to bulletin boards, newsgroups or any other Internet service of any kind without permission from their Manager.
- Run a private business.
- Download any software that does not comply with the Council's Software Policy, this includes shareware, games, screensavers, and 'upgrade patches' available for 'free' on the Internet. Any person could be liable for breaches of copyright where it is directly attributable to their actions. Monitoring procedures built into the Standard Desktop would also quickly identify any unauthorised equipment use.
- Modems must not be attached/installed to networked or stand-alone machines without prior approval from ICT Services; modems may only be attached/installed by ICT Services. Monitoring procedures built into the Standard Desktop would also identify any unauthorised equipment use.

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. If anyone deliberately visits or downloads material from Web Sites containing illegal or unacceptable material they will be dealt with under the Council's disciplinary procedure. The Police may also be notified.

6.6 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 that are available on the intranet:
    - Email Policy.
    - Software Policy.
    - Remote Working Policy.

Unless informed otherwise, the council assumes that all users understand this policy and accept personal responsibility for adhering to its requirements

6.7 Line Manager's Responsibilities

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

- Within an employees work time is relevant to and appropriate to the Council's business and within the context of the users responsibilities.
- Within an employees own time is subject to the rules contained within this document.

6.8 Whom Should I Ask if I Have Any Questions?

In the first instance you should refer questions about this policy to your line manager who will refer you to the ICT Information Security Officer if appropriate. Councillors should refer questions to the ICT Information Security Officer.

You should refer technical queries about the Council's Internet service to the ICT Service Desk.

7 Policy Compliance

Officers of the County Council are required to comply with this policy in respect of its provisions and ethos. Failure to do so may be regarded as a breach of the Officers' Code of Conduct and could result in action being taken against the member of staff concerned.

If you do not understand the implications of this policy or how it may apply to you, seek advice from the ICT Information Security Officer.

8 Policy Governance

The following table identifies who within North Yorkshire County 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	ICT Information Security Officer
Accountable	Senior Information Risk Officer
Consulted	Audit and Information Assurance Manager
Informed	All Council Employees, All Temporary Staff, All Contractors and All Third-party Suppliers.

9 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 ICT Information Security Officer consultation with the Corporate Information Governance Group.

10 References

The following North Yorkshire County Council policy documents are directly relevant to this policy, and are referenced within this document: These policies are available on the corporate intranet

- Email Policy.

- Software Policy.
- ICT Access Policy.
- Remote Working Policy.

The following North Yorkshire County Council policy documents are indirectly relevant to this policy:

- GCSx Acceptable Usage Policy and Personal Commitment Statement.
- Computer, Telephone and Desk Use Policy.
- Removable Media Policy.
- Information Security Incident Management Policy.
- ICT Operational Management Policy.

11 Key Messages

- Users must familiarise themselves with the detail, essence and spirit of this policy before using the Internet facility provided.
- At the discretion of your line manager, and 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).
- Users are responsible for ensuring the security of their computer account username and password. Individual computer account username and passwords should only be used by that individual user, and they should be the only person who accesses their Internet account.
- Users **must not** create, download, upload, display or access knowingly, sites that contain pornography or other “unsuitable” material that might be deemed illegal, obscene or offensive.
- Users must assess any risks associated with Internet usage and ensure that the Internet is the most appropriate mechanism to use.

12 Appendix 1 – Internet Access Bands

Band 0 (24 x 7)	**DEFAULT RESTRICTIONS:** **Access to all websites in .northyorks.gov.uk**
Band 1 (24 x 7)	**Business:** General corporate websites, international and multi-national business corporate websites, Business Associations. **Education**: Education sites – pre, elementary, secondary & high schools, universities. Trade schools, online training, Online teacher resources. **Finance & Investment**: Accountancy, banks, insurance companies. Personal investments & options. Online stock trading. **Government**: all *.gov.uk* sites. Government services – e.g. taxation, armed forces. **Hosting Sites:** Website that host business and individual webs pages. **News**: Newspapers online. Headline news sites, newswire services, personalised news services. Weather sites. **Philanthropic & Professional orgs:** Charity, Environmental, Professional, and Social organisations. **Phishing & Fraud:** Phishing, Phone, service theft advice, Plagiarism and cheating. **Photo Searches:** Resources for photos and images, image hosting, online photo albums. **Politics:** Political sites **Reference**: Personal, professional or educational reference – e.g. dictionaries, maps, language translation. **Religion**: Churches, synagogues & other houses of worship. Faiths & religious beliefs, alternative religions. **Search Engines**: General search engines – e.g. Yahoo, AltaVista, and Google. **Sex Education:** Sites relating to the use of contraceptives, sexual health. **Travel**: Travel destinations, airlines, reservations, discount travel listings, events, sightseeing, weather.
Band 2 (24 x 7)	**Alcohol & Tobacco**: Promotional Web sites, distribution. **Arts & Entertainment**: Movies, TV, music, amusement parks, art galleries, museums, book reviews, horoscopes, performing arts, celebrity fan sites, jokes, comic books, online greetings cards. **Message Boards & Forums:** Newsgroups, opinions or discussion forums. **Kid's Sites:** Child oriented sites and sites published by children. **Computing & Internet**: Reviews, buyer's guides, parts & accessories, software, magazines, web design, Pay-to-Surf sites. **Fashion & Beauty:** Fashion & glamour magazines, Beauty and cosmetics. **Food & Drink**: Recipes, cooking instruction & tips, food products, wine advisors, restaurants, pubs, cafes. Food & Drink magazines and reviews. **Health & Medicine**: General health, fitness & wellbeing. Alternative & complementary therapies. Medical information & reference. Dentistry, optometry & other medical related sites. Support groups. Prescription medicines. **Hobbies & Recreation**: Pastimes – e.g. collecting, gardening. Outdoor recreation – e.g. hiking, camping. Online clubs. Traditional games, role-playing, video games, game reviews – e.g. backgammon, Battleship. Animal/pet related sites. **Job Search & Career Development**: Employment agencies, job listings, career searches. **Motor Vehicles**: Car reviews, vehicle purchases or sales tips, parts catalogues. Motorcycles. Boats. **Real Estate**: Sales listings, rental & relocation services, tips on buying/selling, loans, mortgages, agents. **Shopping**: Online auctions, department stores, market promotions – e.g. clothing, accessories. **Excludes E-Bay.** **Society & Culture**: Home & family related topics – e.g. weddings, births, funerals, gay & lesbian discussions, vegetarianism, naturism, foreign cultures, socio-cultural information. **Sports**: Topics related to sports - e.g. teams, discussion, scores, merchandise, magazines, newsletters, colleges.
Band 3 (24 x 7)	**Advertisements & Pop-Ups:** Banner Ad Servers, Pop-Up advertisements, Adware. **Downloads:** non-streaming movie, video, or sound clips. Downloadable PDA software, Freeware and Shareware, Clip art, Personal storage and back-up. **Illegal Drugs:** Recipes, and instructions for manufacturing, information, distribution, and instruction in the use of illegal substances. **Infrastructure:** Content delivery networks, XML reference schemas, Web analytical and statistical services.
Band 4 (24 x 7)	**Chat:** All Web-based chat software, Instant Message Servers. **Personals & Dating**: and relationship topics – e.g. personal ads, dating services, dating discussions, matchmaking. **Ring tones/Mobile Phone Downloads**: Providers of mobile phone downloads

Band 5 (24 x 7)	**Criminal Activity: Advocate, instruct or give advice on performing illegal acts - e.g. phone/service theft, evading law enforcement, lock-picking, fraud, plagiarism/cheating, burglary techniques.** **Hacking: Promotion, instruction or advice on the illegal use of equipment/software. Instructions or workarounds for filtering software, pirated software and multi-media, computer crime.** **Hate Speech: Propaganda encouraging the oppression of specific groups; or promotion of political or social agendas supremist in nature and exclusionary of others – e.g. racism, or recruitment for membership in a gang or cult.** **SPAM URLS: URLs found in spam, including these topics; computing, finance & Stocks, entertainment, games, health & medicines, humour & novelties and personal & dating.** **Spyware:** Sites that provide or promote information gathering or tracking, malicious executables or viruses, monitoring software. **Tasteless and Offensive:** Offensive or violent language. Excessive use of profanity or obscene gesticulation. **Violence: Portray, describe or advocate physical assault against humans, animals, institutions etc.** **Weapons:** Online purchasing, ordering information, use of weapons – e.g. guns, ammunition, poisons, knifes.
Band 6 (24 x 7)	**Adult/Sexually Explicit:** Adult products, child pornography/paedophilia, explicit cartoons and animation, erotic stories, sexually-orientated or erotic full or partial nudity, depictions or images of sexual acts **Intimate Apparel & Swimwear:** Lingerie, negligee and other intimate apparel modelling, swimwear modelling
Band 7 (24 x 7)	**E-Bay:** Online Auction sit E-Bay and Paypal **Social Networking Sites:** Twitter, Facebook, Bebo, MySpace, Friends Reunited, etc. **Instant Messaging**: MSN, Yahoo, etc. **You Tube:** www.youtube.com
Band 8 (24x7)	**Streaming Media:** Streaming media files or events, internet TV and radio.
Band 9 (24 x7)	**Games:** Game playing or downloading. Game or contest hosting. Tips on games or obtaining cheat codes.
Band 10 (24x7)	**Gambling**: Betting - e.g. bingo, bookmakers, Lottery. Casinos & gambling ventures. Virtual leagues & betting pools.
Always Excluded	**Proxies & Peer-to-Peer, Web-based Email** **Personal Network Storage and Backup**

North Yorkshire County Council

Policy Document PO 35

Non NYCC Network Access

4 May 2013

Document Control

Organisation	North Yorkshire County Council
Title	Non NYCC Network Access Policy
Author(s)	SISCO
Filename	
Owner	SISCO
Subject	Network Access
Protective Marking	Unrestricted
Review date	May 2014

Revision History

Revision Date	Reviser	Version	Description of Revision
01 Feb 2013	SISCO	0.1	Draft of policy edited by SISCO
05 Feb 2013	ICT SMT	0.2	Section 6.1 insert Any variation i.e. length of contract reduced or extended, must be communicated to ICT Services. Section 6.1 insert Each individual must complete the compulsory online Information Security training before any wider access is given. Section 6.7 inserts However, as part of your role within NYCC you may have a legitimate reason to access a site which is blocked. If this is the case you can request access by completing an Internet Access Form.
22 Apr 2013	SISCO	0.3	Review after legal revision Insert definitions for Non-NYCC Individuals –NYCC Network and Information Systems and Service Access Request. Insert location of policies referenced within this policy. Section 6.1 insert Each individual must complete the mandatory Information security online training Insert sect 6.2 Specific approval must be obtained from ICT Services before connecting any non NYCC equipment to the Council's network. Sect 6.4 insert definition of physical security insert sect 6.8 At the discretion of your Responsible Manager, and provided it does not interfere with your work, NYCC permits **personal use of the Internet in your own time** i.e. when you are not being paid (for example during your lunch-break or before and after work).

Document Approvals

This document requires the following approvals:

Sponsor Approval	Name	Date
Senior Information Risk Officer		
Corporate Information Governance Group		

Document Distribution

This document will be distributed to:

Name	Job Title	Email Address

Contents

1. Policy Statement

This document explains the policy and procedure that governs the use of the North Yorkshire County Council Network and Information systems by non NYCC Staff. The policy gives guidance and direction on minimising the risk of data leakage, unauthorised use and the administration of the system

2. Purpose

The purpose of this Policy is to preserve:

- The integrity of the Council's network and systems
- Confidentiality – ensure that all third party users are authorised to use NYCC Network and Information systems and aware of their responsibilities
- Availability – to ensure that NYCC Network and Information systems are made available within a controlled regime to those third parties who require access to NYCC systems
- People dealing with North Yorkshire County Council (NYCC) are entitled to expect that their personal data will be kept fairly and lawfully in line with the Data Protection Act 1998. It is vital that all those engaging with and using NYCC Network and Information systems are aware of this and ensure that a high standard of confidentiality and security is maintained.

3. Scope

This policy applies to all Non NYCC individuals who require access to NYCC computers systems to fulfil their role and the managers responsible for those individuals.

NYCC have a privilege management procedure to ensure that system privileges are properly applied for, granted, managed and controlled. This procedure is required to protect against unauthorised access and the allocation and use of privileges needs to be formally controlled. The policy states that privileges should be allocated on a need-to-use basis, providing the minimum requirement for user's functional roles.

This policy requires Non NYCC Staff to sign a Statement of Compliance & Confidentiality which is included in Appendix 1

4. Definitions & Terms:

Contractor

Any individual, company or organisation external to North Yorkshire County Council who has been employed by the County Council to carry out work or provide a service

Non-NYCC Individuals

A person or persons who are not directly employed by North Yorkshire County Council. These people would be classed as contractors, third party contractors, third party contractor employees etc.

NYCC Network and Information Systems

The communications systems used by NYCC for the management, transfer and receipt of information

Service Access Request (SAR)

A Service Access Request is a form submitted for an employee, contractor, volunteer etc. to enable access to the NYCC Network and Information Systems.

Responsible Manager

Any individual within the County Council employing a contractor

Volunteer

A person who does some act or enters into a transaction without being under any legal obligation to do so and without being promised any remuneration for his/her services

Entering Contracts

A contract is an agreement enforceable at law. Employees may inadvertently enter into contracts or vary terms which the County Council would not like to honour.

Officers must not enter into a contract or vary a term of a contract by using the County Council's email system unless it is authorised by an Assistant Director or higher and is in accordance with the Contract Procedure Rules and/or Procurement Guidelines. A breach of this rule could result in the County Council's Disciplinary Procedure being invoked.

5. Risk

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.

6. Applying the Policy

6.1 Information Security

Contracts with external contractors and/or Third Parties that allow access to the Council's Network and Information systems shall be in operation before access is allowed. These contracts shall ensure that the staff or sub-contractors of the external organisation shall comply with all appropriate security policies

The Responsible Manager for Non NYCC personnel who require access to NYCC Network and Information systems will ensure that the following procedure is adhered to.

Each individual must be given access and the opportunity to read the following policies which expand on the information held within this policy: All ICT policies are available on the corporate intranet

1. PO 26 Email Usage
2. PO 28 Internet Usage
3. PO 01 Information Security

A SAR (Service Access Request) must be completed for each individual outlining the extent of access required, length of time access is required for and the business need for the access

Any variation i.e. length of contract reduced or extended, must be communicated to ICT Services by the responsible manager

Each individual must complete the mandatory Information security online training

6.2 Network Access

Access control rules and procedures are required to regulate who can access the Council information resources or systems and the associated access privileges.

Specific approval must be obtained from ICT Services before connecting any non NYCC equipment to the Council's network.

When a Non NYCC individual leaves the Council, their access to computer systems and data must be suspended at the close of business on the last working day. It is the responsibility of the Responsible Manager to request the suspension of the access rights via the ICT Service Desk.

6.3 Password Security:

All user-level passwords must be changed at a maximum of every 40 days, or whenever a system prompts you to change it. Default passwords must also be changed immediately. If you become aware, or suspect, that your password has become known to someone else, you **must** change it immediately and report your concern to the ICT Service Desk.

It is a user's responsibility to prevent their user id and password being used to gain unauthorised access to Council systems. It is of utmost importance that the password remains protected at all times.

6.4 Physical Security:

Physical security describes security measures that are designed to deny access to unauthorized personnel from physically accessing a building, facility, resource, or stored information. Physical security can be as simple as a locked door

All users must ensure that computers and documents are secured and protected at all times.

The following rules must be adhered to:

- Always lock or log out of your computer if you are away from your desk
- Laptops should always be secured by a locking device

6.5 Email Usage:

The legal status of an email message is similar to any other form of written communication. Consequently, any e-mail message sent from a facility provided to conduct or support official North Yorkshire County Council business should be considered to be an official communication from the Council.

All emails that represent aspects of Council business or Council administrative arrangements are the property of the Council and not of any individual employee.

Emails held on Council equipment are considered to be part of the corporate record and email also provides a record of staff activities.

Non-work email accounts (i.e. personal "home" email accounts such as yahoo, Hotmail etc.) **must not** be used to conduct or support official North Yorkshire County Council business.

Any emails containing RESTRICTED information being sent EXTERNALLY to another Public Sector organisation must be sent from a GCSx email account.

6.6 Monitoring of Email

North Yorkshire County Council maintains its legal right, in accordance with the Regulation of Investigatory Powers Act 2000, to monitor and audit the use of email by authorised users to ensure adherence to Council polices. Users should be aware that deletion of e-mail from individual accounts does not necessarily result in permanent deletion from the Council's ICT systems.

It should also be noted that email and attachments may need to be disclosed under the Data Protection Act 1998 or the Freedom of Information Act 2000. Further information regarding this can be obtained from the Data Management Officer. **You MUST NOT use another person's**

email account login/password/user id/personal security questions. This is strictly forbidden.

Email should not be used for personal business use or to enter into contracts, or be considered defamatory, obscene or for any form of illegal activity which would be considered a criminal offence and/or lead to disciplinary action,

6.7 Internet Usage

The Internet Acceptable Usage Policy should be applied at all times whenever using the Council provided Internet facility.

It is the responsibility of Responsible Managers to ensure that the use of the Internet facility is: Within an employees work time is relevant to and appropriate to the Council's business and within the context of the users responsibilities.

The provision of Internet access is owned by the Council and all access is recorded, logged and interrogated for the purposes of resource management and compliance to current policies and legislation: To help enforce this policy, the council has invested in technology to filter and monitor the usage of its Internet connection.

Those granted access to the internet do so by logging on to the Council's network with their computer username and password.

You are responsible for the security provided by your computer account username and password. Only you should know your username and password and you should be the only person who uses your Internet account.

Access to the Internet via the Council's network is only possible using computers issued by the Council—assembled using standardised hardware and software and connected to the Council's computer network. The *web browser* used by the Council is Microsoft Internet Explorer®.

NYCC systems block websites using URL filtering this includes (but is not exhaustive) websites which are or contain the following material: *Pornographic, illegal, violent, hate and discrimination, offensive, weapons, hacking, web chat, gambling, dating, radio stations, games, streaming media, EBay, YouTube and Social Media Networks i.e. Facebook* However, as part of your role within NYCC you may have a legitimate reason to access a site which is blocked. If this is the case you can request access by completing an Internet Access Form.

6.8 User Responsibilities

As a user of NYCC communication systems it is your responsibility to:

- Know that you may only use the Council's computer network facility within the terms described within this policy. Unless informed otherwise, the Council assumes that all users understand this policy and accept personal responsibility for adhering to its requirements
- Assess any risks associated with Internet usage and ensure that the Internet is the most appropriate mechanism to use
- At the discretion of your Responsible Manager, and provided it does not interfere with your work, NYCC permits **personal use of the Internet in your own time** i.e. when you are not being paid (for example during your lunch-break or before and after work).

7. Policy Compliance

If you do not understand the implications of this policy or how it may apply to you, seek advice from the Data Management Officer or the ICT Senior Information Security Compliance Officer.

8. Policy Governance

Responsible	Senior Information Security Compliance Officer
Accountable	Senior Information Risk Officer
Consulted	Corporate Information Governance Group
Informed	

9. Review and Revision

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

10. Key Messages

- Users are responsible for ensuring the security of their computer account username and password. Individual computer account username and passwords should only be used by that individual user, and they should be the only person who accesses their Internet account or sends/receives email or accesses NYCC systems.
- Users **must not** create, download, upload, display or access knowingly, sites that contain pornography or other "unsuitable" material that might be deemed illegal, obscene or offensive.
- Non-work email accounts **must not** be used to conduct or support official North Yorkshire County Council business.
- Users must ensure that any emails containing Council information must be sent from an official Council email.
- Under no circumstances should users communicate material (either internally or externally), which is defamatory, obscene, or does not comply with the Council's Equal Opportunities policy.
- At the discretion of your Responsible Manager, and provided it does not interfere with your work, NYCC permits **personal use of the Internet in your own time** i.e. when you are not being paid (for example during your lunch-break or before and after work).

11. References

- PO 01 Information Security Policy
- PO 05 ICT Third party relationships policy
- PO 09 IT Access Policy
- PO 26 Email Policy
- PO 28 Internet Usage Policy

Appendices:

Appendix 1 – Confidentiality Agreement

Appendix 1:

Confidentiality Agreement – One Party Obligation

Date: _____

Parties: (1) ("the Recipient")

(2) North Yorkshire County Council ("the Discloser")

RECITALS

(A) Subject to the terms set out in this agreement the Discloser has agreed to divulge Confidential Information (as defined below) to the Recipient relating to the Discloser and its subsidiaries.

(B) The disclosure of confidential information is intended for the purpose of [ ] ("the Purpose")

1. UNDERTAKINGS

The Recipient hereby undertakes with the Discloser (for itself and as trustee for its subsidiaries and shareholders):

1.1 To maintain in the strictest of confidence any Confidential Information presented by the Discloser for the Purpose and not to pass on any such information or make any references towards its existence to any third party;

1.2 Not to use the Confidential Information in any way other than for the Purpose;

1.3 That the Discloser of the Confidential Information shall not be deemed to confer any proprietary rights upon the Recipient to whom the Confidential Information is disclosed;

1.4 Not to reproduce any documentation containing in full or in part any Confidential Information other than that which is necessary to facilitate the Purpose.

1.5 To return on request any extracts, documentation or other material containing or embodying Confidential Information to the Discloser.

2. ACKNOWLEDGEMENT AND CONFIRMATION

The Recipient hereby acknowledges and confirms to the Discloser as follows:

2.1 The Discloser, or any of its employees, subsidiaries, shareholders, agents, officers or advisers, accepts responsibility, liability or warranty, expressed or implied with respect to the accuracy or completeness of the Confidential Information.

2.2 Furthermore no such liability can be raised against the Discloser in relation to any written or oral communication regarding the Confidential Information to the extent that such representation or statement is incorporated into any legally binding contract executed between the parties.

2.3 The provisions of this agreement shall remain in effect without regards for the Recipient withdrawing from any proposed transaction or the destruction or return of the Confidential Information.

2.4 The Recipient agrees that damages alone would not remedy any breach of the provisions within this agreement and accordingly, without prejudice to any and all other rights that the Discloser may have against the Recipient the Discloser will be entitled without proof of special damage to the remedies of injunction, specific performance and other equitable relief for any intended or actual breach of this agreement.

3. EXEMPTION

The above undertakings shall not apply to Confidential Information which:

3.1 Is within or enters the public domain or becomes publicly available other than as a result of a breach of this agreement.

3.2 Becomes lawfully available to the recipient from a third party free from any confidential restriction; or

3.3 The Recipient is required to disclose;

(a) by law;
(b) by any rule or regulation of any stock exchange;
(c) by any court procedure; or
(d) by any rule or regulation of any governmental authority,

Provided that it is practical to do so the Recipient shall consult with the Discloser prior to such disclosure with a view to agreeing its timing and content.

4. DEFINITION OF CONFIDENTIAL INFORMATION

"Confidential Information" shall be regarded as any or all information in whatever form whether disclosed orally or in writing or whether eye readable or machine readable or in any other representation of form including, without limitation, the form, materials and design of any relevant equipment in whole or in part including any associated methods of operation and applications thereof, processes, formulae, plans, strategies, data, designs, specifications, photographs, drawings, technical literature and any related material made available by the Discloser to the Recipient in respect of the Purpose before or after this agreement comes into effect.

5. SEVERANCE

If any provision of this Agreement is held to be invalid or unenforceable, such provision shall be struck out and the remaining provisions shall remain in force.

6. GOVERNING LAW AND JURISDICTION

The provisions hereof shall be governed and construed by English law, and each party agrees to submit to the exclusive jurisdiction of English Courts.

Executed by North Yorkshire County Council

Name:

……

Title:

……

Signature:

……

Executed by (Recipient Party)

Name:

……

Title:

……

Signature:

……

North Yorkshire County Council

Policy Document PO 01

Information Security

01 May 2012

Document Control

Organisation	North Yorkshire County Council
Title	Information Security
Author	ICT Information Security Officer
Filename	Policy
Owner	ICT Information Security Officer
Subject	Information Security
Protective Marking	Unrestricted
Review date	January 2013

Revision History

Revision Date	Revisor	Previous Version	Description of Revision
24/09/2009	ITSO	1.0	Page 3 insert page numbers, Sect 3 delete Information Governance Manager and insert Data Protection Officer. Sect 3 para 5 delete Information Strategy and Governance Committee and insert Strategic Information and Governance Group, insert after annually and recorded within the revision history of the policy. Para 5.21 insert any serious security breaches will be reported to the Information Commissioners Office
09/09/2010	ITSO	1.1	Delete all instances of organisation and replace with council. Delete all instances of Information department and replace with ICT Section 2 para 5 insert printed out or written on paper,
02/11/10	ITSO	1.2	Para 7 insert Officers of the County Council are required to comply with this policy/procedure in respect of its provisions and ethos. Failure to do so may be regarded as a breach of the Officers' Code of Conduct and could result in action being taken against the member of staff concerned'.
25 01 11	ITSO	1.3	Section 5 insert Civil Contingencies Act 2004 into identified risk list and compliance
20.02.12	SMT	1.4	Review by SMT – No changes identified
01 05 12	ITSO	1.5	Review due to PWC audit

Document Approvals

This document requires the following approvals:

Sponsor Approval	Name	Date
Senior Information Risk Officer	Gary Fielding	
Assistant Director of ICT Services		23/09/2009
Audit and Information Assurance Manager	Helen Fowler	24 09 2009

Document Distribution

This document will be distributed to:

Name	Job Title	Email Address

Contents

1. Policy Statement

This top level information security policy is a key component of North Yorkshire County Council overall information security management framework and must be considered alongside more detailed information security documentation including system level security policies, security guidance and protocols or procedures**.** The policy should be read in conjunction with other policies listed in Appendix 1

The aim of information security is to protect the council's information assets from a wide range of threats whether internal or external, deliberate or accidental, in order to ensure business continuity and minimise the impact of adverse events on customers and staff.

2 Purpose

The objectives of this Policy are to preserve:

- Confidentiality - Access to Data shall be confined to those with appropriate authority.
- Integrity – Information shall be complete and accurate. All systems, assets and networks shall operate correctly, according to specifications.
- Availability - Information shall be available and delivered to the right person, at the time when it is needed and in the relevant format.

The aim of this policy is to establish and maintain the security and confidentiality of information, information systems, applications and networks owned or held by the council by:

- Ensuring that all employees and members are aware of and fully comply with the relevant legislation. As described in this and other policies.
- Describing the principals of security and explaining how they shall be implemented in the council.
- Information includes data printed out or written on paper, stored on computers, transmitted across networks, sent by fax, stored on tapes and disks or spoken in conversation and over the telephone.
- To introduce a consistent approach to security ensuring that all employees and members fully understand their responsibilities.
- Creating and maintaining within the organisation a level of awareness of the need for Information Security as an integral part of the day to day business.
- Protecting information assets under the control of the council

3. Scope

This policy applies to all information, information systems, networks, applications and locations in North Yorkshire County Council

Ultimate responsibility for information security rests with the Senior Information Risk Officer of the council, but on a day-to-day basis the Information Security Officer and the Data Protection Officer shall be responsible for managing and implementing the policy and related procedures and associated policies.

4. Definitions

Information System (IS)

An Information System is defined as a system that requires the use of and the support of the council's ICT infrastructure and/or a system that stores or manipulates data and/or any system that requires on going support from the ICT department

System Owner (SO)

The System Owner (SO) is the individual who has overall responsibility for an information system, its governance and usage.

System Administrator (SA)

The System Administrator (SA) is responsible for the day to day maintenance of the system. This is separated from the system owner role however both roles may be done by the same person.

System User (SU)

Individuals who access and use the information system to perform tasks defined within their access roles and privileges.

5. Risks

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.

The Council is obliged to abide by all relevant UK and European Union legislation. The requirement to comply with this legislation shall be devolved to employees of the council, who may be held personally accountable for any breaches of information security for which they may be held responsible. The council shall comply with the following legislation and other legislation as appropriate

The Data Protection Act (1998)
The Data Protection (Processing of Sensitive Personal Data) Order 2000.
The Copyright, Designs and Patents Act (1988)
The Computer Misuse Act (1990)
The Health and Safety at Work Act (1974)
Human Rights Act (1998)
Regulation of Investigatory Powers Act 2000
Freedom of Information Act 2000
Health & Social Care Act 2001
Health & Social Care Act 2008
EU Directive on Privacy and Electronic Communications (2006)
Mental Health Act 1983
Mental Health Act 2007
Disability Discrimination Act (DDA) 1995
Disability Discrimination Act (DDA) 2005
Electronic Communications Act 2000
Intellectual Property Act 1994
Civil Contingencies Act 2004

Other legal statutes brought into force after this document is printed will also apply without exception.

6 Applying the Policy

6.1 Management of Security

The Information Security Officer shall be responsible for implementing, monitoring, documenting and communicating security requirements for the council.

Line Managers are responsible for ensuring that their permanent and temporary staff and contractors are aware of:-

The information security policies applicable in their work areas
Their personal responsibilities for information security
How to access advice on information security matters

All staff shall comply with information security procedures including the maintenance of data confidentiality and data integrity.

The Information Security Policy shall be maintained, reviewed and updated by the Corporate Information Governance Group. This review shall take place annually and be recorded within the revision history of the policy

Line managers shall be individually responsible for the security of their physical environments where information is processed or stored

Each member of staff shall be responsible for the operational security of the information systems they use.

Each system user shall comply with the security requirements that are currently in force and identified within the system specific policy, and shall also ensure that the confidentiality, integrity and availability of the information they use is maintained to the highest standard.

Contracts with external contractors that allow access to the council's information systems shall be in operation before access is allowed. These contracts shall ensure that the staff or sub-contractors of the external organisation shall comply with all appropriate security policies

6.2 Information Security Awareness Training

Information security awareness is included in the staff induction process.

An ongoing awareness program has been established in order to ensure that staff awareness is refreshed and updated as necessary. Online training is available to all staff

6.3 Contracts of Employment

Staff security requirements shall be addressed at the recruitment stage

6.4 Security Control of Assets

Each IT asset, (hardware, software, application or data) shall have a named custodian who shall be responsible for the information security of that asset.

6.5 Access Controls

Only authorised personnel who have a justified and approved business need shall be given access to restricted areas containing information systems or stored data.

6.6 User Access Controls

Access to information shall be restricted to authorised users who have a bona-fide business need to access the information.

6.7 Computer Access Control

Access to computer facilities shall be restricted to authorised users who have a business need to use the facilities.

6.8 Application Access Control

Access to data, system utilities and program source libraries shall be controlled and restricted to those authorised users who have a legitimate business need
Authorisation to use an application shall depend on the availability or procurement of a license from the supplier

6.9 Equipment Security

In order to minimise loss of, or damage to, all assets, equipment shall be physically protected from threats and environmental hazards.

6.10 Computer and Network Procedures

ICT are responsible for ensuring management of computers and networks are controlled through standard documented procedures that have been authorised

6.11 Information Risk Assessment

The core principle of risk assessment and management requires the identification and quantification of information security risks in terms of their perceived value of asset, severity of impact and the likelihood of occurrence.

Once identified, information security risks shall be managed on a formal basis by ICT. They shall be recorded within a baseline risk register and action plans shall be put in place to effectively manage those risks. The risk register and all associated actions shall be reviewed at regular intervals. Any implemented information security arrangements shall also be a regularly reviewed feature of the councils risk management program. These reviews shall help identify areas of continuing best practice and possible weakness, as well as potential risks that may have arisen since the last review was completed.

6.12 Information security incidents and weaknesses

All information security events and suspected weaknesses are to be reported to the Information Security Officer. All information security events shall be investigated to establish their cause and impacts with a view to avoiding similar events.

6.13 Classification of Sensitive Information.

A consistent system for the classification of information within Government organisations enables common assurances in information partnerships, consistency in handling and retention practice when information is shared with non-government bodies

The council shall implement appropriate information classifications controls, based upon the results of formal risk assessment and guidance contained within the Information Governance Toolkit to secure their information assets.

The Information Security Officer or Data Protection Officer should be contacted for further guidance and instruction.

6.14 Protection from Malicious Software

The organisation shall use software countermeasures and management procedures to protect itself against the threat of malicious software. All staff shall be expected to co-operate fully with this policy. Users shall not install software on the council's property without permission from ICT.

6.15 User media

Removable media of all types that contain software or data from external sources, or that have been used on external equipment, require the approval of ICT before they may be used on council systems Such media must also be fully virus checked before being used on the council's equipment.

6.16 Monitoring System Access and Usage

An audit trail and log will be kept of all monitoring that is undertaken

The council has in place routines to regularly audit compliance with this and other policies. In addition it reserves the right to monitor activity where it suspects that there has been a breach of policy. The

Regulation of Investigatory Powers Act (2000) permits monitoring and recording of employees' electronic communications (including telephone communications) for the following reasons

- Establishing the existence of facts
- Investigating or detecting unauthorised use of the system
- Preventing or detecting crime
- Ascertaining or demonstrating standards which are achieved or ought to be achieved by persons using the system (quality control and training)
- In the interests of national security
- Ascertaining compliance with regulatory or self-regulatory practices or procedures
- Ensuring the effective operation of council systems

Any monitoring will be undertaken in accordance with the above act and the Human Rights Act (1998)

6.17 Accreditation of Information Systems

The council shall ensure that all new information systems, applications and networks include a security plan and are approved by ICT before they commence operation.

All system owners should develop a system specific policy prior to any system going live in order to distinguish between the security management considerations and requirements of the system. Specific responsibilities must be assigned and obligations communicated directly to those who use the system.

6.18 System Change Control

Changes to information systems, applications or networks shall be reviewed in line with the change control policy. ICT must be involved in this process.

6.19 Intellectual Property Rights

The council shall ensure that all information products are properly licensed and approved by ICT. It is the responsibility of system owners to work with ICT to ensure this takes place.

Users shall not install software on the council's property without permission from ICT

6.20 Business Continuity and Disaster Recovery Plans

The council shall ensure that business impact assessment, business continuity and disaster recovery plans are produced for all mission critical information, applications, systems and networks

7. Policy Compliance

Officers of the County Council are required to comply with this policy in respect of its provisions and ethos. Failure to do so may be regarded as a breach of the Officers' Code of Conduct and could result in action being taken against the member of staff concerned.

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 the Information Security Officer.

ICT and the Information Security Officer shall keep the Corporate Information Governance Group and senior management informed of the information security status of the council by means of regular reports and presentations any serious security breaches will be reported to the Information Commissioners Office once approved by the Senior Information Risk Officer

8. Policy Governance

The following table identifies who within the 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	ICT Information Security Officer
Accountable	Senior Information Risk Officer
Consulted	Audit and Information Assurance Manager, Corporate Information Governance Group
Informed	All Council Employees, All Temporary Staff, All Contractors and All Third-party Suppliers.

This policy shall be subject to audit by internal and external auditors.

9. 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 Security Officer in consultation with the Corporate Information Governance Group.

10. References

The following council policy documents are directly relevant to this policy, and are referenced within this document:

- GCSx Acceptable Usage Policy and Personal Commitment Statement.
- Software Policy.
- ICT Access Policy.
- Internet Usage Policy.
- Computer, Telephone and Desk Use Policy.
- Remote Working Policy.
- Portable Media and Encryption Policy.
- Information Security Incident Management Policy.
- Employee Guide to Information Security
- Email Policy
- IT Asset Policy
- Use of IT Equipment Policy
- Acceptable use Policy
- Incident Policy
- Mobile Working Policy
- Disaster Recovery Policy
- Business Continuity Policy
- Risk Assessment Policy
- Remote Access Policy
- Disposal/ Recycling Policy

The following legislation is pertinent to this policy

- The Data Protection Act (1998)
- The Data Protection (Processing of Sensitive Personal Data) Order 2000.
- The Copyright, Designs and Patents Act (1988)
- The Computer Misuse Act (1990)
- The Health and Safety at Work Act (1974)
- Human Rights Act (1998)
- Regulation of Investigatory Powers Act 2000
- Freedom of Information Act 2000
- Health & Social Care Act 2001
- Health & Social Care Act 2008
- Mental Health Act 1983
- Mental Health Act 2007
- The European Union (EU) Directive 2002/58/EC Directive on Privacy and Electronic Communications
- Disability Discrimination Act (DDA) 1995
- Disability Discrimination Act (DDA) 2005
- Electronic Communications Act 2000
- Intellectual Property 1994

11. Key messages

- Users shall not install software on the council's property without permission from ICT
- All information security events and suspected weaknesses are to be reported to the Information Security Officer
- Each member of staff shall be responsible for the operational security of the information systems they use
- Only authorised personnel who have a justified and approved business need shall be given access to restricted areas containing information systems or stored data.

North Yorkshire County Council

Policy Document PO 05

Third Party and Contractors Relationships

02 May 2012

Document Control

Organisation	North Yorkshire County Council
Title	Third Party and Contractor Relationships
Author	ITSO
Filename	Policy
Owner	ICT Information Security Officer
Subject	External Staff
Protective Marking	Unrestricted
Review date	January 2013

Revision History

Revision Date	Revisor	Previous Version	Description of Revision
4 Jan 2011	ITSO	1.0	Remove all instances of Charlotte Wright and replace with Operations manager.
16 May 2011	ITSO	1.1	Insert ICT Senior Management Team as approvals.
16 Jun 2011	ITSO	1.2	Remove all instances of ICT Operations Manager and replace with correct title of Head of ICT Operations
20 Feb 012	SMT	1.3	Review by SMT – No changes identified
02 May 2012	ITSO	1.4	Review due to PWC audit

Document Approvals

This document requires the following approvals:

Sponsor Approval	Name	Date
Assistant Director of ICT Services		18/03/10
Head of ICT Operations		
ICT Senior Management Team		

Document Distribution

This document will be distributed to:

Name	Job Title	Email Address

Contributors

Contents

1 Policy Statement

Information and information systems are important corporate assets and it is essential to take all the necessary steps to ensure that they are at all times protected, available and accurate to support the operation and continued success of ICT Services North Yorkshire County Council.

ICT Services acknowledges that we must demonstrate to third parties our expertise in security technology and implementing it. To achieve this it is recognised that we must protect our own assets as well as the environment.

The aim of the Council's Information Security Policy, Security Standards and Information Security Manual is to maintain the confidentiality, integrity and availability of information stored, processed and communicated by and within the Council. These standards, procedures and policies are used as part of the information security management system (ISMS) within ICT Services.

This policy outlines the way ICT Services works with trusted third parties and contractors.

The following procedures are covered:

- Computer hardware and peripherals
- Software support
- Cleaning services

2 Purpose

2.1 Third parties

Before a third party can engage in business with the ICT Services a confidentiality agreement must be signed by the third party if they need to access the network or Council systems for any reason. This will not apply if it is written into a formal contract. Any violation of this agreement may result in North Yorkshire County Council taking legal action. A copy of the current confidentiality agreement is at Appendix A.

All third party personnel must be escorted at all times whilst in the ICT Services. In the event of third parties requiring access to the Data Centre, the Head of ICT Operations will arrange that they are escorted at all times. The escort must ensure that all confidential information is protected, for example turning off display monitors not in use and ensuring consoles that are not in use are locked.

No third party contractor shall be given access to the Council network unless authorised by the relevant Responsible Manager.

In the event that a server needs to be taken off site by a third party, the Head of ICT Operations must ensure that all of the Council's critical information is removed before hand over.

For further information on the relationships between ICT Services and third parties, please refer to the Head of ICT Operations who holds the contract and service level agreements.

In the event that software needs to be tested this will be carried out in a controlled environment and under the supervision of a permanent member of staff.

In the event that software needs to be passed over to a third party for further off site testing, The Head of ICT Operations must ensure that all of the Councils critical information is backed up prior to its removal.

The cleaning contractors do not have permission to enter the Data Centre or any communications cabinets; it is the responsibility of the Server Team Leader (Infrastructure), to ensure the Data Centre is kept in a presentable and safe state.

This includes but is not limited to:

- Disposing of boxes/packaging from hardware/software.
- Ensuring food and drinks are not taken into the Data Centre.
- Ensuring books/manuals and documentation are filed and locked away after use.

2.2 Contractors

Suitable information security awareness, training and education shall be provided to all contractors, clarifying their responsibilities relating to the Council's Information Security Policy Acceptable Use Policy, Email Policy and Internet Policy,

The Responsible manager is responsible for determining the access rights to information and systems and for authorising the appropriate access permissions to the contractor. If granted privileged access rights the contractor must sign the use of privileged access statement and return this statement to the Information Security Officer

Contractors will be issued with a temporary ID card. It is the contractor's responsibility for safe guarding this card and protecting it from unauthorised use. ID cards are to be worn at all times and be visible

The Responsible Manager is to ensure that the contractor is fully aware of the County Council and the contractor's responsibilities and obligations in regards to compliance to all aspects of the Health and Safety at work act 1974

Prior to starting work all contractors are to be informed of emergency procedures that are in place this must include evacuation in the event of a fire or bomb alert, contact telephone numbers, the location of first aid facilities. If working in the data centre contractors must be made aware of the fire suppressant system deployed in the centre

Contractors are required to report to their relevant Responsible Manager prior to starting work

Contractors are to ensure that any property issued to them is returned upon completion of their employment

Contractors should raise any concerns they have in relation to their contractor activity with their Responsible Manager; this may include but is not limited to county council procedures and protocols, contract management or any short comings they identify

A contractor induction pack is available from the administration office. This pack includes

- Information Security Policy
- Email Policy
- Internet Usage Policy
- Confidentiality statement
- Use of privileged access policy

Before being issued with a contractor ID card these documents must be read and relevant statements signed to acknowledge compliance

3 Scope

This policy applies to all external third parties and contractors providing a service to ICT Services

4 Definition

4.1 Definitions Glossary

Contractor Any individual, company or organisation external to North Yorkshire County Council who has been employed by the County Council to carry out work or provide a service

Responsible manager any individual within the County Council employing a contractor

5 Policy Governance

Responsible	ICT Information Security Officer
Accountable	Assistant Director ICT Services
Consulted	ICT Senior management Team
Informed	All ICT Service Employees, All Temporary Staff, All Contractors and All Third-party Suppliers.

6 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 ICT Information Security Officer and ICT Senior Management Team.

7 References

The following North Yorkshire County Council policy documents are directly relevant to this policy, and are referenced within this document:

Email Policy
Information Security Policy
Internet Usage Policy

Confidentiality Agreement – One Party Obligations

Date: _____

Parties: (1) ("the Recipient")

(2) ICT Services
North Yorkshire County Council ("the Discloser")

RECITALS

(A) Subject to the terms set out in this agreement the Discloser has agreed to divulge Confidential Information (as defined below) to the Recipient relating to the Discloser and its subsidiaries.

(B) The disclosure of confidential information is intended for the purpose of [ ] ("the Purpose")

1. UNDERTAKINGS

The Recipient hereby undertakes with the Discloser (for itself and as trustee for its subsidiaries and shareholders):

1.1 To maintain in the strictest of confidence any Confidential Information presented by the Discloser for the Purpose and not to pass on any such information or make any references towards its existence to any third party;

1.2 Not to use the Confidential Information in any way other than for the Purpose;

1.3 That the Discloser of the Confidential Information shall not be deemed to confer any proprietary rights upon the Recipient to whom the Confidential Information is disclosed;

1.4 Not to reproduce any documentation containing in full or in part any Confidential Information other than that which is necessary to facilitate the Purpose.

1.5 To return on request any extracts, documentation or other material containing or embodying Confidential Information to the Discloser.

2. ACKNOWLEDGEMENT AND CONFIRMATION

The Recipient hereby acknowledges and confirms to the Discloser as follows:

2.1 The Discloser nor any of its employees, subsidiaries, shareholders, agents, officers or advisers accept responsibility, liability or warranty, expressed or implied with respect to the accuracy or completeness of the Confidential Information.

2.2 Furthermore no such liability can be raised against the Discloser in relation to any written or oral communication regarding the Confidential Information to the extent that such representation or statement is incorporated into any legally binding contract executed between the parties.

2.3 The provisions of this agreement shall remain in effect without regards for the Recipient withdrawing from any proposed transaction or the destruction or return of the Confidential Information.

2.4 The Recipient agrees that damages alone would not remedy any breach of the provisions within this agreement and accordingly, without prejudice to any and all other rights that the Discloser may have against the Recipient the Discloser will be entitled without proof of special damage to the remedies of injunction, specific performance and other equitable relief for any intended or actual breach of this agreement.

3. EXEMPTION

The above undertakings shall not apply to Confidential Information which:

3.1 Is within or enters the public domain or becomes publicly available other than as a result of a breach of this agreement.

3.2 Becomes lawfully available to the recipient from a third party free from any confidential restriction; or

3.3 The Recipient is required to disclose;

(a) by law;
(b) by any rule or regulation of any stock exchange;
(c) by any court procedure; or
(d) by any rule or regulation of any governmental authority,

Provided that it is practical to do so the Recipient shall consult with the Discloser prior to such disclosure with a view to agreeing its timing and content.

4. DEFINITION OF CONFIDENTIAL INFORMATION

"Confidential Information" shall be regarded as any or all information in whatever form whether disclosed orally or in writing or whether eye readable or machine readable or in any other representation of form including, without limitation, the form, materials and design of any relevant equipment in whole or in part including any associated methods of operation and applications thereof, processes, formulae, plans, strategies, data, designs, specifications, photographs, drawings, technical literature and any related material made available by the Discloser to the Recipient in respect of the Purpose before or after this agreement comes into effect.

5. SEVERANCE

If any provision of this Agreement is held to be invalid or unenforceable, such provision shall be struck out and the remaining provisions shall remain in force.

6. GOVERNING LAW AND JURISDICTION

The provisions hereof shall be governed and construed by English law, and each party agrees to submit to the exclusive jurisdiction of English Courts.

Executed by North Yorkshire County Council

Name:

……

Title:

……

Signature:

……

Executed by (Recipient Party)

Name:

……

Title:

……

Signature:

……

North Yorkshire County Council

Policy Document PO 09

ICT Access Policy

02 May 2012

Document Control

Organisation	North Yorkshire County Council
Title	ICT Access Policy
Author	ICT Information Security Officer
Filename	NYCC ICT Access Policy
Owner	ICT Information Security Officer
Subject	ICT policy
Protective Marking	Unrestricted
Review date	March 2013

Revision History

Revision Date	Revisor	Previous Version	Description of Revision
13/08/09	C Wright	1.0	Added information on requesting system access
08/09/09	ITSO	1.1	Sections 5 para 3 insert Legal compliance. additional notes inserted into key messages
14/09/09	ITSO	1.2	Document approvals insert Chief Information Officer. Section 9 table responsible insert ICT Information Security Officer, accountable insert Assistant director for ICT
23/04/12	SMT	1.3	Page 4 line 5 council I should be council. Section 6.1.1 Weak & Strong Passwords - This section may now be at odds with the current Information Security e-Learning as the training now lists 4 types of characters which can be used in a strong password and states that 3 of the 4 should be used. Section 6.11 reads ' sent to the ICT Services' should this be 'sent to ICT Services', Section 7 refers to Information Security Officer changed to Senior Information Security Compliance Officer (SISCO), same in the Responsible grid and section 9. With the roll-out of Windows 7 strong passwords will be enforced
02/05/12	ITSO	1.4	Review due to PWC audit

Document Approvals

This document requires the following approvals:

Sponsor Approval	Name	Date
Senior Information Risk Officer		
Assistant Director for ICT Services		29/09/2009
Corporate Information Governance Group		

Document Distribution

This document will be distributed to:

Name	Job Title	Email Address

Contributors

Contents

1 Policy Statement

North Yorkshire County Council has specific requirements for protecting information and information systems against unauthorised access. The need to ensure the data on the council network and the network availability operate within a safe and confidential environment is of the utmost importance to the council

The council will effectively communicate the need for information and information system access control. The council has a responsibility to preserve integrity in order to protect the network from unauthorised or accidental modification and to preserve confidentiality in order to protect assets against unauthorised use or disclosure

2 Purpose

Information security is the protection of information against accidental or malicious disclosure, modification or destruction. Information is an important, valuable asset of the council which must be managed with care. All information has a value to the council However, not all of this information has an equal value or requires the same level of protection.

Access controls are put in place to protect information by controlling who has the rights to use different information resources and by guarding against unauthorised use.

Formal procedures are in place to control how access to information is granted and how such access is changed.

This policy also mandates a standard for the creation of strong passwords, their protection and frequency of change.

This policy exists to safeguard the council's computer network and associated corporate information systems from unauthorised access and applies to all functions within the council used for:

- The storage, sharing and transmission of data.
- The printing or scanning of data or images.
- The provision of internet systems for receiving, sending and storing data and images.

.

The overall purpose of the policy is to ensure the security of these information resources

3 Scope

This policy applies to all North Yorkshire County Council Councillors, Committees, Departments, Partners, and Employees of the Council (including system support staff with access to privileged administrative passwords), contractual third parties and agents of the council with any form of access to the council information and information systems.

4 Definition

Access control rules and procedures are required to regulate who can access the council information resources or systems and the associated access privileges. This policy applies at all times and should be adhered to whenever accessing council information in any format, and on any device.

5 Risks

On occasion business information may be disclosed or accessed prematurely, accidentally or unlawfully. Individuals or companies, without the correct authorisation and clearance may intentionally or accidentally gain unauthorised access to business information which may adversely affect day to day business. This policy is intended to mitigate that risk.

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**.**

Where relevant the council will always ensure it complies with the following legislation (correct at date of ratification):

- Copyright, Designs and Patents Act 1998
- Access to Health Records Act 1990
- Computer Misuse Act 1990
- The Data Protection Act 1998
- The Human Rights Act 1998
- Electronic Communication Act 2000
- Regulation of Investigatory Powers Act 2000
- Freedom of Information Act 2000
- Health & Social Care Act 2001
- EU Privacy and Monitoring Directives Act 2003
- Sexual Offenders Act 2003

6 Applying the Policy - Passwords

6.1 Choosing Passwords

Passwords are the first line of defence for our ICT systems and together with the user ID help to establish that people are who they claim to be.

A poorly chosen or misused password is a security risk and may impact upon the confidentiality, integrity or availability of our computers and systems.

6.1.1 *Weak* and *strong* passwords

A *weak password* is one which is easily discovered, or detected, by people who are not supposed to know it. Examples of weak passwords include words picked out of a dictionary, names of children and pets, car registration numbers and simple patterns of letters from a computer keyboard.

A *strong password* is a password that is designed in such a way that it is unlikely to be detected by people who are not supposed to know it, and difficult to work out even with the help of a computer.

Everyone must use strong passwords with a minimum standard of:

- At least seven characters.
- Contain a mix of alpha and numeric, with at least one digit
- More complex than a single word (such passwords are easier for hackers to crack).

The Government advises using Environ passwords with the following format: consonant, vowel, consonant, consonant, vowel, consonant, number, number. An example for illustration purposes is provided below:

- pinray45

6.2 Protecting Passwords

It is of utmost importance that the password remains protected at all times. The following guidelines must be adhered to at all times:

- Never reveal your passwords to anyone.
- Never use the 'remember password' function.
- Never write your passwords down or store them where they are open to theft.
- Never store your passwords in a computer system without encryption.
- Do not use any part of your username within the password.
- Do not use the same password to access different North Yorkshire County Council systems.
- Do not use the same password for systems inside and outside of work.

6.3 Changing Passwords

All user-level passwords must be changed at a maximum of every 40 days, or whenever a system prompts you to change it. Default passwords must also be changed immediately. If you become aware, or suspect, that your password has become known to someone else, you **must** change it immediately and report your concern to the ICT Service Desk.

Users **must not** reuse the same password within 20 password changes.

6.4 System Administration Standards

The password administration process for individual council systems is well-documented and available to designated individuals.

All council IT systems will be configured to enforce the following:

- Authentication of individual users, not groups of users - i.e. no generic accounts.
- Protection with regards to the retrieval of passwords and security details.
- System access monitoring and logging - at a user level.
- Role management so that functions can be performed without sharing passwords.
- Password admin processes must be properly controlled, secure and auditable.

6.5 Applying the Policy – Employee Access

6.6 User Access Management

Formal user access control procedures must be documented, implemented and kept up to date for each application and information system to ensure authorised user access and to prevent unauthorised access. They must cover all stages of the lifecycle of user access, from the initial registration of new users to the final de-registration of users who no longer require access. Each user must be allocated access rights and permissions to computer systems and data that:

- Are commensurate with the tasks they are expected to perform.

- Have a unique login that is not shared with or disclosed to any other user.
- Have an associated unique password that is requested at each new login.

User access rights must be reviewed at regular intervals to ensure that the appropriate rights are still allocated. System administration accounts must only be provided to users that are required to perform system administration tasks.

6.7 User Registration

A System Access Request (SAR) for access to the Council's computer systems must first be submitted to the ICT Service Desk for processing. Applications for access must only be submitted if approval has been gained from your line manager and ICT Client Officer.

A copy of the SAR form for corporate and GCSX system access is available on the council's intranet.

When an employee leaves the council, their access to computer systems and data must be suspended at the close of business on the employee's last working day. It is the responsibility of the line manager to request the suspension of the access rights via the ICT Service Desk.

6.8 User Responsibilities

It is a user's responsibility to prevent their userid and password being used to gain unauthorised access to council systems by:

- Following the Password Policy Statements outlined above in Section 6.
- Ensuring that any computer they are using that is left unattended is locked or logged out.
- Leaving nothing on display that may contain access information such as login names and passwords.
- Informing the ICT Service Desk of any changes to their role and access requirements.

6.9 Network Access Control

Specific approval must be obtained from ICT Services before connecting any equipment to the council's network.

6.10 User Authentication for External Connections

Where remote access to the council network is required, an application must be made via the ICT Service Desk. Remote access to the network must be secured by two factor authentication consisting of a username and a secure token. For further information please refer to the Remote Working Policy.

6.11 Supplier's Remote Access to the Council Network

Partner agencies or 3rd party suppliers must not be given details of how to access the Council's network without permission from ICT Services. Any changes to supplier's connections must be immediately sent to the ICT Services so that access can be updated or ceased. All permissions and access methods must be controlled by ICT Services.

Partners or 3rd party suppliers must contact ICT Services before connecting to the council network and a log of activity must be maintained. Remote access software must be disabled when not in use.

6.12 Operating System Access Control

Access to operating systems is controlled by a secure login process. The access control defined in the User Access Management section (section 7.1) and the Password section (section 6) above must be applied. The login procedure must also be protected by:

- Not displaying any previous login information e.g. username.
- Limiting the number of unsuccessful attempts and locking the account if exceeded.
- The password characters being hidden by symbols.
- Displaying a general warning notice that only authorised users are allowed.

All access to operating systems is via a unique login id that will be audited and can be traced back to each individual user. The login id must not give any indication of the level of access that it provides to the system (e.g. administration rights).

System administrators must have individual administrator accounts that will be logged and audited. The administrator account must not be used by individuals for normal day to day activities, please refer to the ICT Services Privilege Management Policy.

6.13 Application and Information Access

Access within software applications must be restricted using the security features built into the individual product. The directorate system administration team of the software application is responsible for granting access to the information within the system. The access must:

- Be compliant with the User Access Management section (section 7.1) and the Password section (section 6) above.
- Be separated into clearly defined roles.
- Give the appropriate level of access required for the role of the user.
- Be unable to be overridden (with the admin settings removed or hidden from the user).
- Be free from alteration by rights inherited from the operating system that could allow unauthorised higher levels of access.
- Be logged and auditable.

7 Policy Compliance

Officers of the council are required to comply with this policy in respect of its provisions and ethos. Failure to do so may be regarded as a breach of the Officers' Code of Conduct and could result in action being taken against the member of staff concerned.

If you do not understand the implications of this policy or how it may apply to you, seek advice from Information Security Officer.

8 Policy Governance

The following table identifies who within North Yorkshire County 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	ICT Information Security Officer
Accountable	Senior Information Risk Officer
Consulted	Audit and Information Assurance Manager, Corporate Information Governance Group
Informed	All NYCC staff, contractors and third-parties.

9 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 ICT Information Security Officer

10 References

The following North Yorkshire County Council policy documents are directly relevant to this policy, and are referenced within this document:

- Remote Working Policy.
- ICT Services Privilege Management Policy

The following North Yorkshire County Council policy documents are indirectly relevant to this policy:

- Email Policy.
- Internet Usage Policy
- Software Policy.
- GCSx Acceptable Usage Policy and Personal Commitment Statement.
- Computer, Telephone and Desk Use Policy.
- Removable Media Policy.
- Information Security Incident Management Policy.
- ICT Operational Management Policy.

11 Key Messages

- All users must use **strong** passwords.
- Passwords must be protected at all times and must be changed at least every 40 days.
- User access rights must be reviewed at regular intervals.
- It is a user's responsibility to prevent their userid and password being used to gain unauthorised access to Council systems.
- Partner agencies or 3rd party suppliers must not be given details of how to access the Council's network without permission from ICT Services
- Partners or 3rd party suppliers must contact ICT Services before connecting to the North Yorkshire County Council network.
- The Council will take seriously and investigate all security breaches concerning
    - Abuse of Internet\email including accessing inappropriate sites
    - Sharing of Passwords\inappropriate access to corporate or personal information
    - Unauthorised modification of systems
    - Deleting another users files
    - Introduction of viruses to the network
    - Inappropriate disclosure of information
    - Use of unauthorised software or devices