'Happy children aiming high!'

New Hartley First School

'A very caring and nurturing school in which the well-being of every child is paramount.'
'The quality of education continues to be good.'
Ofsted, June 2016

E-mail Usage Policy

Status:	**Statutory**
Created/Reviewed	**Summer 2012, 2014, 2016**
Next Review:	**Summer 2018**

Introduction

This document sets out the School policy, which is directly in line with Northumberland Council's policy, towards the use of email.

The purpose of this Policy is to describe the acceptable use of the Council's email system, and its operation and management.

Any queries arising from this Policy or its implementation can be taken up directly with the Information Security Officer at ITSecurity@northumberland.gov.uk

The Information Security Officer is the Owner of this document and has approved management responsibility for its development, review and evaluation.

Summary of Contents:

1. Scope

1.1 This Policy applies to all elected Members, employees, students, members of the public or any other person operating e-mail systems provided by Northumberland County Council or using Council premises for this purpose.

1.2 The policy should be read in conjunction with the Council's Code of Conduct and the ICT & Information Security Policy. These documents are available on the Intranet, or from the Information Security Officer at ITSecurity@northumberland.gov.uk

2. Introduction

2.1 Northumberland County Council provides Outlook email accounts available to all employees with access to a computer.

2.2 Although it is acknowledged that circumstances may arise when it is permissible for employees to send and / or receive personal emails, these facilities are primarily for business use.

3. Responsibilities

3.1 To protect individual officers and councillors and the Council itself from any potential embarrassment or liability, the contents of this Policy must be strictly adhered to by all users. Failure to do so may constitute an offence and would be dealt with in accordance with the Council's disciplinary process.

3.2 Upon termination or suspension of employment by either the Council or the employee, for whatever reason, it is the responsibility of the HR department to inform Information Services in order to disable the employee's network access and email account. Mailbox and data files will still be available for examination should this be required.

3.3 Any employee who accesses or attempts to access another user's mailbox without either management or employee authorisation, or following termination or suspension of employment, will be subject to disciplinary procedures.

4. Monitoring

4.1 As a responsible email provider, the Council will subject all transmitted and received email to filtering; this may result in a relatively brief delay in transmission of emails between the Council's network and any partners' networks.

4.2 It should also be borne in mind that while the email system is very reliable it cannot be seen as providing guaranteed delivery. Options such as Delivery Reports should be used if evidence is required that an email has been successfully received.

4.3 All messages may be monitored for compliance with this Policy, and in exceptional circumstances such as fraud investigations or disciplinary investigations, email accounts may be accessed, read and the

information used without the knowledge of the User, and in compliance with the Human Rights Act 1998.

4.4 When Email facilities have been set up the Control Panel settings for Mail must only be changed, if necessary, by someone from Information Services, or in accordance with instructions provided by Information Services.

4.5 Any improper use of internal or external email, as defined in this policy or otherwise, will be considered by the Council to be potentially a disciplinary matter.

4.6 A computer must not be left unattended without either shutting it down or using a screen saver with password protection or locking the computer. Any Email sent from a computer will be sent under the name of the person logged on to the network irrespective of who actually typed and physically sent the message. Users may be held responsible for all communications issued under their name whilst logged on to the network.

5. Shared computers

5.1 All access to the Email system will be through the use of the User's network login ID and password.

5.2 Users are responsible for all email activity carried out using their network login ID, and any email sent will have their details as the sender. Therefore, a user must log off from the machine before moving away.

5.3 Any attempt to logon using another person's ID may be regarded as a disciplinary matter.

6 Access to Email Accounts by Third Parties

6.1 All Outlook Calendars will be accessible to all other users, in order to enable the setting up of meetings etc.

6.2 All users must enable read-only access to their inbox for a colleague and/or manager. This ensures that important emails are not missed and can be progressed at times of unplanned absence. Users accessing another inbox in these circumstances must comply with the requirements below at 6.5.4.

6.3 There are circumstances under which access to email accounts in addition to or as an alternative to paragraph 6.2 may be granted to third parties in the absence of the employee – normally an appropriate manager. These circumstances are described below, and all employees must be aware that such access may take place.

6.4 <u>Planned Absence</u>

6.4.1 In cases of planned absence such as annual leave, an employee may apply permissions on their email account to allow a

colleague or manager to access or share their email account. See Paragraph 6.2 above.

6.4.2 As a minimum employees must always apply an Out-Of-Office message during periods of absence.

6.4.3 Information Services Service desk on (01670 53)3333 can advise on how to set these permissions and apply an Out-Of-Office message.

6.4.4 Any queries regarding accessing or sharing email accounts may be addressed to the Information Security Officer on 01670 533309 or at ITSecurity@northumberland.gov.uk

6.5 Unplanned Absence

Where access to an absent user's email account is required in addition to or as an alternative to Paragraph 6.2, the following procedure should be followed:

6.5.1 Where absence is unplanned and therefore unexpected, requests for access to an absent employee's email account must be made by the employee's line manager to the Information Security Officer by email at ITSecurity@northumberland.gov.uk

6.5.2 The Information Security Officer will require the circumstances of the absence and a business reason for the request for access. This information will be confirmed with the department's Chief Officer or appropriate representative of the department.

6.5.3 Wherever possible the line manager must inform the employee that this access will take place, or at least make and document clear attempts to do so.

6.5.4 Those with access to the account should avoid opening clearly personal emails, and wherever possible restrict themselves to opening only those emails required for immediate business purposes. See Paragraph 9 for information on personal use.

6.5.5 Access of this kind may be to a specific email, the entire mailbox, or may apply appropriate Outlook permissions to named individual / s depending on the circumstances and business requirements.

6.5.6 Access may also be granted to files and folders in an employee's H:Drive.

6.6 The decision on all these kinds of requests for access will rest with the Information Security Officer. If access is denied for any reason, appeal by the line manager can be made through the Chief Executive.

6.7 Any employee who accesses or attempts to access another user's mailbox without either management or employee authorisation, or following termination or suspension of employment, will be subject to disciplinary procedures.

7. E Mail Content and Layout

7.1 All Email must include the approved signature –

Name
Job Title
Team or Unit Name
Group/Department/Service/Team
Northumberland County Council
****
************ NE/TD** ******

Telephone: *** ********
E-mail ……@northumberland.gov.uk
Web site: www.northumberland.gov.uk

The signature can also include post-nominal letters and/or logos representing qualifications and/or membership of relevant organisations and bodies.

7.3 The following message will be added automatically to each Email – *"If this is delivered to you in error would you please destroy all copies of it immediately and contact the sender".*

7.4. At all times Users sending an Email must bear in mind that it will be seen to have been sent on behalf of the Council and as such the Council could be liable for any action resulting from the Email.

8. Acceptable use of Email

8.1 The Council is the owner of all emails and attachments sent using Council equipment and resources.

8.2 The Council prohibits the use of Email for purposes which may be illegal or the creation of Email messages whose content may be offensive. Email has a legal status and in relevant circumstances Users may wish to consider if they could defend what they have written in a court of law before sending it.

8.3 Email facilities must not be used for:

8.3.1 The creation, downloading, transmission or receiving of any illegal, obscene, indecent, immoral, defamatory or racist images, data or other material, or any data capable of being resolved into obscene or indecent images or material

8.3.2 The creation, downloading, transmission or receiving of material which is designed or likely to cause annoyance, inconvenience or needless anxiety to any other Users

8.3.3 The transmission of material which may infringe the copyright of another person, or material that is protected by trade secret

8.3.4 The transmission of unsolicited commercial or advertising material

8.3.5 The unsolicited sending of inappropriate e-mail to large numbers of people, via Outlook or on the Internet

8.3.6 Deliberate activities which result in the corruption or destruction of other Users' data, violating the privacy of other Users or disrupting the work of other Users

8.3.7 Activities which deny or restrict service to other Users such as the overloading of access links or switching equipment

8.3.8 Activities which compromise, or have the potential to compromise networked resources, such as the introduction of viruses

8.4 If a user receives an email which is obscene, defamatory or in any other way contravenes the points above, s/he must not forward it to another address. Distribution of such emails may be considered to be a disciplinary matter. The email should be deleted. If a similar email is received from the same sender, Information Services should be informed in order to filter email from this source, and carry out any investigation as may be appropriate.

8.5 Users should avoid automatically using delivery and receipt options. These should only be used when required, the additional network traffic created by them having the potential to impact on the response time of the system.

8.6 Users should exercise care when copying or forwarding emails to other and multiple addresses, as doing so may result in unauthorised or inappropriate disclosure of the information to third parties. Emails, particularly those containing large attachments, sent to multiple addresses can also create unnecessary pressure on the capacity of the email system.

8.7 All users must be aware that the content of emails may be released in response to requests for information under the Freedom of Information Act or the Data Protection Act. Caution should therefore be exercised, in particular when making reference to third parties.

8.8 The Council reserves the right to retain information relating to email usage for a period of up to 2 years.

8.9 Internal Email

8.9.1 All Users must ensure that they are authorised to send each Email taking into account its content and recipient.

8.9.2 It is always advisable to check the recipient's identity and the accuracy of their email address before sending the Email to ensure that the correct person has been selected. This is

particularly important when sending sensitive or confidential information or documents.

8.9.3 The appropriate level of formality must be observed and the use of email must not be trivialised.

8.10 External Email

8.10.1 All Users must ensure that they are authorised to send each Email taking into account its content and recipient. Employees must not send any Email message binding the Council to any position, agreeing any term or making any admission unless they are authorised to do so.

8.10.2 Employees must not give advice to third parties via Email unless authorised to do so and after having fully considered their own and the Council's potential liability.

8.10.3 The appropriate level of formality must be observed, use of email must not be trivialised and it must include the recognised "Email signature" as described at Paragraph 7.1

8.10.4 Users are advised to ensure that they provide their email address accurately to others. The Council's email system will not generate invalid address notifications to those who email to an inaccurate address.

9. Personal Use

9.1 Personal use of email accounts is similar to the kind of use identified in the Staff Code of Conduct on telephone use. The Email system is primarily for business purposes, although it is recognised that there will be occasions when reasonable levels of personal use is justified.

9.2 Any personal email should contain the word "PERSONAL" in the subject line to identify them as such should exceptional circumstances require a mailbox to be accessed as described at paragraphs 4.3 and 6 above.

9.3 The sending of jokes, games and unauthorised software, either internally or externally, is prohibited.

9.4 Email facilities must not be used in connection with any secondary business activities unless approved as part of any formal Council scheme.

9.5 As with business use, personal use of the email system will be monitored as described at paragraph 4 above.

10. Attachments

10.1 <u>Outgoing Attachments</u>

10.1.1 As file size affects the service being provided, the size of email attachments should not exceed a maximum of 10MB. If this is too restrictive alternative means are available from Information Services Service Desk on (01670 53)3333 or at cshelpdesk@northumberland.gov.uk

10.1.2 Users must also note that emails containing large attachments sent to multiple recipients can adversely affect network capacity and performance.

10.1.3 Users should also be aware that third party companies systems may have lower limits set for emails received.

10.2 Incoming Attachments

10.2.1 Users are advised that extractions from external Emails must be saved onto the machines hard drive (C: drive) and virus checked before being opened.

10.2.2 If there is any doubt about the authenticity of an email, or the contents of an attachment, it should not be opened, and advice should be sought from the Information Services Service Desk on (01670 53)3333

10.2.3 A number of file types are deleted by the Email system on receipt, usually those associated with application or executable files, batch and script files, and sound and video. Problems associated with attachments with these file types should by addressed to the Information Services Service Desk on (01670 53)3333

11. Unsolicited Email

11.1 All Email users have a responsibility to ensure that they are using the correct means of notification.

11.2 The mass Emailing of messages and/or attachments is not allowed except in exceptional circumstances as agreed in advance with the department representative. A Bulletin Board is maintained on the intranet which allows for notifications/messages/information intended for general staff distribution.

12. Email Account Management

12.1 Retaining Emails on the server for longer than necessary is an inappropriate use of the Email server, and too many Emails left on the server will degrade the service generally. The email system will automatically remove emails older than 2 years.

12.2 The maximum size of a User's email mailbox is 1GB including sent and deleted items, and email users are responsible for managing this resource in the most efficient and effective way.

12.3 When Emails are no longer needed they must be deleted as soon as possible, from the Inbox, Sent Items and Deleted Items. Care must be taken over this however, as once an Email is deleted it will probably be irrecoverable.

12.4 If an Email needs to be saved, the equivalent of backup, it must be transferred to the Users H:Drive. Users should contact the Information Services Service Desk on (01670 53)3333 for information on this.

12.5 The content of emails is subject to retrieval for the purpose of Freedom of Information or Data Protection requests. Users must therefore bear in mind that emails must be stored efficiently, be easily identified and retrieved, and be kept accurate and up to date. This is particularly important with regard to personal data.

12.6 Email attachments should be saved to an appropriate folder on the user's H:Drive immediately on receipt and removed from the email system.

12.7 PST (Personal folder files) must only be created for purposes agreed with Information Services, generally for offline copying of a mailbox.

12.8 The network will require a password change every 90 days. Any accounts with no activity during a 90 day period will be disabled. A further 90 day period of inactivity will result in the account being deleted. An appropriate manager will be informed, and an offline backup copy of any data can be created if required.

13 Sending Confidential Information

13.1 Confidential information is one of the Council's most valuable assets and disclosure may harm the Council or any individuals identified by the information.

13.2 In very general terms, confidential information can be said to be any data which is not generally available to the public. It may therefore include personal information, payroll data, contract and tendering information etc.

13.3 Documents of a highly confidential nature must not be transmitted by e-mail, or any other means, without appropriate authorisation from a senior manager. See the Transportation, Transfer and Sharing of Data Policy for more information

13.4 Any document sent as ordinary text to external Email addresses can be easily read if intercepted before reaching the intended recipient. Therefore it is important that Users take this into account before sending any sensitive or confidential information or documents.

13.5 Internal Email on the Council server is recognised as secure. However, Email leaving the Council is not so secure and action appropriate to the document or information being sent must be taken. See the Transportation, Transfer and Sharing of Data Policy for more information.

14. Points to Remember

14.1 Think before writing
14.2 Always be polite
14.3 Check the content of the message
14.4 Be concise
14.5 Check recipient's properties (if internal)
14.6 Include the disclaimer on all external Email (automatic from central Email server)
14.7 Include the standard signature at the end of all Email