EAST AYRSHIRE COUNCIL

POLICY & RESOURCES COMMITTEE

18th April 2007

ACCEPTABLE USE POLICY GOVERNING THE PERSONAL USE OF COMMUNICATIONS SYSTEMS

Report by Depute Chief Executive / Executive Director of Corporate Support

1. PURPOSE OF REPORT

1.1 To seek approval for the implementation of an "Acceptable Use Policy governing the Personal Use of Communications Systems".

2. BACKGROUND

2.1 In April 2007, Internal Audit conducted an assignment, reference CA/05/1002, entitled "Internet and e.Mail Monitoring Arrangements".

2.2 The principle recommendation and subsequent commitment arising from this assignment was for the development of a revised Policy in respect of personal Staff / Members use of Internet / e.Mail, and the publication of an associated set of guidance for users.

2.3 In this respect the Head of IT and the Head of Personnel have developed a new "Acceptable Use Policy governing the Personal Use of Communications Systems" which is attached as Appendix A of this Report. In due course, this Policy will be supplemented by a user handbook which will be issued to all staff / Members who access the Internet, use the Council's e.mail system, and/or use the Council's telephone network.

2.4 The new Policy covers all Council staff, including teaching staff, Members and Community Representatives, who access the Internet, use the Council e.mail system, and/or use the Council's telephone network.

3. MAIN ASPECTS OF NEW POLICY

3.1 The main aspects in regards to the new Policy are ;

- All Staff, Members and Community Representatives will have access to the Internet and the Council e.mail system, and will have the ability to e.mail out-with the Council.

- All Staff and Members will have access to the Council's telephone network.

- Staff and Members will no longer be charged for personal use of Internet access or the Council's e.mail system, but should continue to reimburse the Council for personal telephone use.

- Other than in cases of emergency, personal use of these facilities will be restricted to lunch breaks and/or periods pre and post-normal working day.

- Executive Directors / Heads of Service retain the right to deny or withdraw Internet and/or e.mail access at any time.

- All Staff, Members and Community Representatives, including current users, will be required to sign an "Acceptance and Declaration to Comply" with the terms of the Policy.

- All Internet access will be automatically monitored with monthly usage reports issued to Executive Directors / Heads of Service as appropriate.

- All External e.mails will be automatically monitored with monthly usage reports highlighting inappropriate use issued to Executive Directors / Heads of Service as appropriate.

- All Internal e.mails will be automatically monitored with monthly usage reports highlighting inappropriate use issued to Executive Directors / Heads of Service as appropriate.

4. ACCEPTANCE AND DECLARATION TO COMPLY

4.1 All staff, Members and Community Representatives, including current users, will be required to sign an "Acceptance and Declaration to Comply**"** with the terms of the Policy. A copy of the Declaration can be viewed at the back of the appended Policy.

4.2 Copies of the Policy and the Declaration will be made available for download from the Staff Intranet, and Departments / Services will be required to collate signed copies of the Declaration for retention within individual personnel files.

5. MONITORING ARRANGEMENTS

5.1 All Internet access, together with all internal and external e.mails, will be automatically monitored for inappropriate use. All Internet access will be reported monthly to Executive Directors / Heads of Service, as appropriate. In respect of e.mail, in-appropriate use and instances of excessive traffic volumes will reported back to Executive Directors / Heads of Service, as appropriate.

5.2 When the new Policy comes into effect, a "warning" screen, a copy of which is attached as Appendix B to this report, will appear each time a user logs onto the Council network.

6. TRADES UNION AGREEMENT

6.1 Arrangements are in place to seek the agreement of the Trades Unions in respect of the new Policy.

7. TIMESCALES

7.1 Subject to approval of the new Policy, it is anticipated that the necessary processes and ICT system changes will be in place to permit a "go-live" date of 1st May 2007.

8. LEGAL / POLICY IMPLICATIONS

8.1 Nil.

9. FINANCIAL IMPLICATIONS

9.1 There are no financial implications arising from the implementation of the new Policy other than for Executive Directors to note that staff and Members will no longer be charged for personal use of the Internet and the Council's e.mail system.

10. RECOMMENDATIONS

10.1 It is recommended that Committee approves the "Acceptable Use Policy governing the Personal Use of Communications Systems".

Elizabeth Morton
Depute Chief Executive / Executive Director of Corporate Support

LIST OF BACKGROUND PAPERS

Nil.

For further information on this Report, please contact Malcolm Roulston,
Head of Information Technology (Tel : 01563 576809).

AMR / March 2007

APPEXDIX B

Internet Access & E.Mail Warning Screen

EAST AYRSHIRE COUNCIL

INTERNET ACCESS & ELECTRONIC MAIL & TELEPHONY

Systems for monitoring Internet access, both internal and external e.mail messaging, and telephony are currently operational.

Staff must not deliberately access inappropriate web sites hosting illegal content, or which contain material which is obscene, violent or discriminatory.

Staff must not transmit e.mail messages which contain inappropriate content such as profanity or inappropriate images.

Improper use of Internet access, e.mail messaging and / or telephony may result in disciplinary action or legal proceedings.

Please refer to the Acceptable Use Policy governing the Personal Use of Communications Systems.

I agree to the terms of the Acceptable Use Policy governing the Personal Use of Communications Systems

Click ok to proceed

ACCEPTABLE USE POLICY
GOVERNING THE USE OF COMMUNICATION SYSTEMS

ALL NETWORK USERS

Teachers, Community Representatives, Elected Members and Corporate Users

ACCEPTABLE USE POLICY
GOVERNING THE USE OF COMMUNICATION SYSTEMS

ACCEPTABLE USE POLICY
GOVERNING THE USE OF COMMUNICATION SYSTEMS

2 Document Control

2.1 Version History

Author	Date	Version	Approved By	Date Approved
Ian Aston	2/4/2007	1.1.1		

ACCEPTABLE USE POLICY
GOVERNING THE USE OF COMMUNICATION SYSTEMS

3 Introduction

3.1 Overview

We view the internet, email and telephony as essential tools, however, their use can expose the Council to technical, commercial and legal risks if they are not used sensibly. The aim of this policy is to:

- Provide guidance on use of the internet, email and telephony at work to minimise East Ayrshire Council's exposure to these risks
- Explain what users can and cannot do
- Provide information on all monitoring systems in use
- Explain the consequences for users and East Ayrshire Council if users fail to follow the rules set out in this policy
- Provide basic housekeeping guidelines and recommendations

This document has been created in order to protect East Ayrshire Council, and all users, from the following risks relating to its network resources:

User Productivity

- East Ayrshire Council does allow personal use of its network resources. This activity is restricted to lunch breaks and periods before or after the normal working day. Users must follow the same restrictions with regards to 'appropriate use' as and when they are using network resources for business reasons.

Enhance Network Bandwidth

- Non-productive sites and emails consume a significant amount of bandwidth. When users download large graphics, audio clips, movie clips or other non-work related information, it puts a drain on the Council's limited bandwidth which is an expensive resource. Eventually this causes a slowdown in network performance which impacts other users attempting to complete work related tasks via the internet.

Reduce Legal Liability

- This Acceptable Use Policy must be followed to protect the Council and all users from legal liability relating to internet, email and telephony use

ACCEPTABLE USE POLICY
GOVERNING THE USE OF COMMUNICATION SYSTEMS

It is important that all users read this policy very carefully. Breaches of this policy will be taken very seriously. If there is anything in this policy that users do not understand it is up to them to contact their line manager / supervisor / head teacher for an explanation.

ACCEPTABLE USE POLICY
GOVERNING THE USE OF COMMUNICATION SYSTEMS

4 Acceptable Use Policy

4.1 General Acceptable Use Policy

Inappropriate or malicious use of East Ayrshire Council's resources include:

- Inappropriate use or sharing of East Ayrshire Council IT privileges or resources (such as logon account information, access to PC, access to printer etc)
- Unauthorised changing of another user's password or access rights
- Violations or infringes on the rights of any other person, including the right to privacy
- Creating or transmitting defamatory, false, inaccurate or otherwise biased material
- Using an East Ayrshire Council resource to actively engage in displaying, procuring or transmitting material that is in violation of sexual harassment policy or laws, hostile workplace laws or other legal policies
- Transmitting of customer, partner or other business confidential data
- Distributing, disseminating or storing images, text or materials that might be considered indecent, pornographic, profane, threatening, racially offensive, abusive, obscene, terrorist or illegal
- Undertaking deliberate activities that waste user effort or networked resources
- Any activity that restricts or inhibits other users from using the system or the efficiency of computer systems
- Any communication that encourages the use of controlled substances
- Any communication that uses the system for the purpose of criminal intent
- The installation of applications without prior approval
- The use of internet chat applications (eg/ MSN Messenger)
- Introducing any form of computer virus onto the network
- Users may not illegally copy material protected under copyright law or make that material available to others for copying

4.2 Internet Usage

East Ayrshire Council has a policy for the use of the internet whereby users must ensure that they:

ACCEPTABLE USE POLICY
GOVERNING THE USE OF COMMUNICATION SYSTEMS

- Use the internet in an acceptable manner
- Do not create unnecessary business risks to the Council by their misuse of the internet

Unacceptable Behavior

In particular, the following examples are deemed unacceptable use of the internet:

- Visiting internet sites that contain obscene, hateful or pornographic material
- Using the computer to perpetrate any form of fraud, software or music piracy
- Using the internet to send offensive or harassing material to other users
- Downloading commercial software or any copyrighted materials belonging to third parties, unless this download is covered or permitted under a commercial agreement or other such licence
- Hacking and attempting to hack into unauthorised areas
- Undertaking deliberate activities that waste user's effort or networked resources
- Use of Peer to Peer File Sharing Applications, including applications to download and share music or videos over the internet

If users inadvertently access inappropriate material they should inform their line manager / supervisor / head teacher immediately. This information should then be relayed to the ICT Security Manager.

Users should exercise extreme caution if conducting financial transactions or disclosing personal information over the internet and are reminded that the Council will not be responsible for any damages or loss that they may suffer.

Users should be aware that instant messaging is specifically forbidden (applications including, but not restricted to : MSN Messenger, AOL Instant Messenger, Yahoo Messenger etc)

4.3 Email Usage

East Ayrshire Council has a policy for the use of email whereby users must ensure that they:

ACCEPTABLE USE POLICY
GOVERNING THE USE OF COMMUNICATION SYSTEMS

- Use email in an acceptable way
- Do not create unnecessary business risk to the Council by their misuse of the email system

Email is the principal communication method by which the Council conducts business. Given its importance to the business, users are expected to adhere strictly to the policy.

Unacceptable Behavior

In particular, the following examples are deemed unacceptable use of email:

- Use of the Council communications system to set up personal businesses
- Use of the Council communications system to send chain letters
- Forwarding of Council confidential data to external locations, this includes personal email accounts. If a role dictates that a user must transfer confidential material offsite, users must do so using an encrypted USB flash drive (see section 7.6 for additional information)
- Accessing copyrighted information in a way that violates the copyright
- Breaking into the system or unauthorised use of a password / mailbox
- Broadcasting unsolicited personal views on social, political, religious or other non-business related matters
- Transmitting unsolicited commercial or advertising material
- Give rise to an unauthorised contractual commitment on behalf of the Council

Users should think twice before giving out their east-ayrshire.gov.uk *(or indeed any)* email address. Special regard should be given to entering it on a website or some form of “discussion list”. Users should be mindful of the reputation of the organisation that they are dealing with, for instance, by deciding whether or not they have been established for some time.

4.4 Telephone Usage (including mobiles and faxes)

Business Use - users of the Council's telephone systems are authorised to use the telephone system in support of their individual duties, departmental and service needs.

ACCEPTABLE USE POLICY
GOVERNING THE USE OF COMMUNICATION SYSTEMS

Personal Use - it is recognised that, from time to time, it may be necessary for users to make use of Council telephone / fax facilities for reasons unrelated to their role within the Council. In doing so, users should adhere to the following guidance:

Personal Use – No reimbursement to Council

- Personal use of facilities may be made in appropriate circumstances e.g. emergency situations; to check on relative/dependant who is ill; to notify others of overtime arrangements; returning call from relative/dependent etc
- Wherever possible or practicable, personal use should be within the user's own time, such as during recognised work breaks or during teachers non-class contact time
- Where it is not possible for calls to be made outside normal working hours, users should endeavour to ensure that disruption to their work, and the work of others, is kept to a minimum
- Where personal use of facilities is made in appropriate circumstances there shall be no cost to the user

Personal Use - Reimbursement to Council

- It is anticipated that from time to time users may make personal use of facilities in other circumstances e.g. contacting bank; arranging appointments etc.
- Personal use in such circumstances must be within the user's own time, such as lunch breaks and periods before or after the normal working day
- The user shall be required to reimburse the Council for the use of facilities (see Appendix III)

4.5 Word Processing And Other Software

Any limited personal use of East Ayrshire Council software, for example Microsoft Office applications such as Microsoft Word, should conform to the following model:-

- In the current environment, the "H:\" drive is private to most users
- If users store files on networked drives they should be aware that these files will be backed up. Any file that has been backed up can be

restored if required (for example: when the original file becomes corrupt or is deleted). Any files stored on the computers' local drive (typically C:\) will NOT be backed up and, therefore, cannot be restored

- IT Services recommend that users store all personal files and file sub-folders on their private "H:\" drive, under a file folder called "Personal". Note that this does not prevent East Ayrshire Council from investigating the contents of such personal files, in exceptional circumstances, if gross misconduct or criminal activity is suspected

ACCEPTABLE USE POLICY
GOVERNING THE USE OF COMMUNICATION SYSTEMS

5 Privacy And Monitoring

5.1 Overview

The internet, email and telephony are valuable business tools. However, misuse of these facilities can have a negative impact upon user productivity and the reputation of the Council.

All of the Council's system resources are provided for business purposes, therefore users can have no expectation of privacy. The Council maintains the right to examine any systems and inspect any data recorded on those systems. Although personal use of the Council's IT systems is acceptable, users expressly waive any right of privacy in anything they create, store, send or receive using the Council's computer equipment or via internet access. Users consent to allow authorised Council personnel to access and review all materials created, stored, sent or received by the user through any Council equipment, network or internet connection. Furthermore, all content on the Council's email system remains the property of the Council.

In order to ensure compliance with this policy, the Council also reserves the right to use monitoring software in order to check upon the use and content of IT devices and communication.

5.2 Internet Monitoring

The Council shall monitor access to the internet by providing reports to all Heads of Service at the beginning of every month. These reports detail websites visited, the duration of time spent on each website, the total amount of time spent online for the duration of the report (typically covering a one month period), frequency of visits to websites and the time / date of each visit. Users are reminded that personal activity should be restricted to lunch breaks and periods before or after the normal working day.

The Council has also purchased specialist software that will enable inappropriate sites to be blocked and automatically scan web sites for inappropriate content as they are being accessed by the user (see Appendix I).

These monitoring arrangements apply to both business and personal use of internet.

All logfiles will be kept for a period of 2 years. Under the Data Protection Act, users are entitled to inspect log files. Should any user require to do this, they should consult with their line manager or contact the Council's Data Protection Officer.

The discovery of any unauthorised use may result in suspension of internet access and / or disciplinary action (see section 6 for additional information).

5.3 Email Monitoring

The Council shall monitor email usage by using recognised software to automatically scan all incoming, outgoing and internal email messages for viruses and for pre-defined content (see Appendix II).

Email messages that are found to contain any of the pre-defined content detailed in Appendix II will be quarantined automatically. Quarantined emails are regularly scanned by a team of email administrators within IT. All appropriate emails are then released. Inappropriate emails are held on the system for a maximum of 62 days. The Council shall provide reports to all Directors at the beginning of every month. These reports detail all inappropriate outgoing and internal emails, listing the email sender, subject and reason for quarantine (ie: profanity, inappropriate image, chain mail etc). The Director will then be required to investigate the matter, taking action as appropriate.

These monitoring arrangements apply to both business and personal use of email and apply to all incoming, outgoing and internal use of the email system.

The discovery of any unauthorised use may result in suspension of email access and/ or disciplinary action (see section 6 for additional information).

5.4 Telephone Monitoring

The Council shall monitor the usage of telephones by providing reports to Heads of Service, summarising the calls made from telephone extensions. This facility is available for digital exchanges serving the main Council locations and it is anticipated that this will be extended over time. Where there are reasonable grounds on which to suspect misuse of the telephone

system, more detailed reports on numbers called and the duration of calls from telephone extensions shall be made available.

Details of numbers called and the duration of calls made from mobile telephones are automatically received from mobile phone providers.

The Council will not record the contents of any telephone calls. The only exceptions to this rule are calls to Council's Telephone Helplines. These calls are monitored and recorded for business purposes. The users providing this service are aware of these monitoring arrangements.

These monitoring arrangements apply to both business and personal use of telephones.

The discovery of any unauthorised use may result in suspension of telephony access and/ or disciplinary action (see section 6 for additional information).

ACCEPTABLE USE POLICY
GOVERNING THE USE OF COMMUNICATION SYSTEMS

6 Responses To Breaches Of Policy

6.1 Overview

Users that fail to comply with or uphold these policies are likely to be subject to disciplinary action, as set out in the Council's Disciplinary Policy. Furthermore, if, following due process, the Council is satisfied that gross misconduct has occurred as a result of a user's contravention of any of these policies, the result will normally be that the user is summarily dismissed. This means termination of the employment contract without notice, payment in lieu of notice, or compensation of any kind.

Users violating these provisions, applicable national laws or Council procedures or policies are subject to:

- loss of network privileges, including internet and / or email access and / or telephony access
- Council's Disciplinary procedures including dismissal, if appropriate
- Criminal prosecution, if appropriate

As these policies cannot anticipate every situation, users are responsible for seeking guidance from an appropriate person (usually the line manager / supervisor / head teacher / IT account manager) on any issue not covered by the policy.

If a user suspects any breach of this, or any, policy in their workplace they should report their concerns to their line manager / supervisor / head teacher, IT Account Manager, Internal Audit or the ICT Security Manager.

ACCEPTABLE USE POLICY
GOVERNING THE USE OF COMMUNICATION SYSTEMS

7 Housekeeping

7.1 Recommendations

Please be aware of the following guidelines:

- All important email messages should be filed or stored in a personal folder on the central file server (see 'EMAIL PERSONAL FOLDERS' on page 61 of the current ICT Security Handbook for advice)
- If a user receives a wrongly delivered email they should redirect it to the correct person. If the email message contains confidential information they must not make use of that information and must not disclose it. If the email contains inappropriate material they should inform their line manager / supervisor / head teacher immediately. This information should then be relayed to the ICT Security Manager
- Do not subscribe to email services that result in emails being sent automatically, unless these are useful for the role
- Do not send out trivial or personal email messages. These lead to congestion of the system and reduce it's efficiency
- Make messages as informative as possible
- Be polite, for example: when writing email messages the use of capital letters is technically considered to be the equivalent of SHOUTING
- Do not transmit confidential or other sensitive information via internet email
- Use caution when revealing personal information such as your address or phone number (or those of others)
- Avoid sending excessively large email attachments (attachments over 10MB in size)
- Do not use email to harass or threaten anyone in any manner, for example: the persistent sending of unwanted email may be viewed as harassment

7.2 Password Selection

All users are required to authenticate themselves on the Windows network to log on to all internal systems. A dialog box will appear at logon, prompting that the device should only be accessed by authorised personnel.

ACCEPTABLE USE POLICY
GOVERNING THE USE OF COMMUNICATION SYSTEMS

All users are required to change their password the very first time they logon. This is automatically enforced. Users are then required to change their passwords every 42 days thereafter. Passwords should be at least 8 characters long and contain 3 of the following: a number, a lowercase character, an uppercase character or an extended character. For example: Sun$h1n3, £1Sh0pper, £$ecretS and £Glasg0w are all considered 'strong' passwords (and are therefore difficult to guess / crack)

7.3 Trojans, Virii and Spyware

East Ayrshire Council have several levels of virus protection. Anti-virus signatures are updated hourly on systems with an active network connection. On other systems, anti-virus signatures are updated every time they connect to the Council network. However, these products are not fail safe (i.e./ it is possible to get a computer virus before an update has been published by the vendor).

All users must exercise caution when dealing with email attachments and internet downloads and should seek advice from the IT Helpdesk if they are unsure.

Intentionally introducing malicious programs onto the network will be considered a very serious offence and may be dealt with by disciplinary action.

7.4 Security & Asset Security

East Ayrshire Council equipment should be cared for at all times, both the cost of replacing the item and the cost of the information that the item contains should be taken into account. The equipment remains the responsibility of the person allocated to it at all times. Please take note of the following guidelines:

- Where possible, ensure that the screen does not face a public view and that the PC is locked when unattended. Users are responsible for ensuring that their PC is locked, even if they are only leaving their desk for a few moments. To lock a PC: press CTRL-ALT-DEL and click the LOCK COMPUTER button. Alternatively, press and hold the WINDOWS icon key on the keyboard and press the L key. Users are

responsible for the security of their computer and must not allow use by any unauthorised persons (including fellow work colleagues)
- All portable equipment (eg/ USB flash drives, mobile phones, laptops, HP iPaqs) should not be left unattended in plain view whether in or outside the office
- Portable equipment should be secured if possible at all times (eg/ mobile phones and iPaqs locked with a PIN, laptops locked with a BIOS password), protecting the device and the stored content

When taking portable devices offsite, users should ensure that they are stored securely at all times. Use the following as guidelines:

- Do not leaves phones, laptops, iPaqs and other equipment in a car unattended
- Always keep a laptop out of sight when stored in a car, even if the user is in the car with it
- Never leave the laptop unattended in a public place
- If a user takes their laptop with them to eat in a public place, secure the laptop from being snatched (eg/ place the shoulder strap under the chair leg)
- Never put a laptop in hold luggage, carry it on the plane as hand luggage

Users should also adhere to the following security measures:

- Do not under any circumstances disclose your password to any other person
- Do not impersonate another user when sending an email
- Do not amend email messages received
- If a user identifies a security problem, notify IT immediately
- Take every reasonable precaution to protect the Council's network from security issues such as computer viruses
- Do not show or identify a security problem to others
- Do not allow another person to use your account
- Ensure that you are familiar with the contents of the IT Security User Code of Practice, copies of which are available from IT Services
- Under no circumstances should software be installed on ICT facilities except in accordance with your IT Account Manager

ACCEPTABLE USE POLICY
GOVERNING THE USE OF COMMUNICATION SYSTEMS

7.5 HP iPaq Security

Setting up security on an iPaq simply means creating a password that must be entered whenever the unit is turned on. Without the correct password, no one will be able to access files / emails or use the iPaq. To set up a password, please refer to the 'Setting up security on an HP iPaq' policy, available from IT Services.

7.6 USB Flash Drive Security

At the moment, there are no procedures directly relating to the use of USB flash drives. The last published ICT Security Staff Booklet is dated 2001, before flash drives came into widespread use. An updated version of this booklet is expected later this year (2007). However, there are several points that users should note:

- Content on the flash drive will only be scanned for virii when copied to / from the drive or when a file is opened from the drive
- The flash drives should be purchased by EAC
- The flash drives must hold the data in encrypted format
- The flash drives should hold EAC data only, no personal files should be kept on the memory stick. Flash drives for personal use must not be used on East Ayrshire Council PCs
- While we are confident that we have complete virus protection on each East Ayrshire Council PC, each user has a responsibility to ensure that no virus is introduced on to a Council system

ACCEPTABLE USE POLICY
GOVERNING THE USE OF COMMUNICATION SYSTEMS

Appendix I – Internet Content Filter Categories

The following table is provided as a reference to highlight which categories of websites are permitted and prohibited by East Ayrshire Council. The Council reserves the right to amend these categories without prior notice.

Category	Blocked	Allowed
Adult & Sexually Explicit	✓	
Advertisements	✓	
Arts & Entertainment		✓
Business & Economy		✓
Chat	✓	
Computing & Internet		✓
Criminal Skills	✓	
Drugs, Alcohol & Tobacco	✓	
Education		✓
Finance & Investment		✓
Food & Drink		✓
Gambling	✓	
Games		✓
Glamour & Intimate Apparel	✓	
Government & Politics		✓
Hacking & Remote Proxy	✓	
Hate Speech	✓	
Health & Medicine		✓
Hobbies & Recreation		✓
Hosting Sites		✓
Job Search & Career Development		✓
Lifestyle & Culture		✓
Motor Vehicles		✓
News		✓
Personal Web Sites		✓
Personals & Dating	✓	
Real Estate		✓
Reference		✓
Religion		✓
Search Engines		✓
Sex Education		✓

ACCEPTABLE USE POLICY
GOVERNING THE USE OF COMMUNICATION SYSTEMS

Shopping		✓
Sports		✓
Streaming Media		✓
Travel		✓
Usenet News		✓
Weapons & Violence	✓	
Web Based Email	✓	

ACCEPTABLE USE POLICY
GOVERNING THE USE OF COMMUNICATION SYSTEMS

Appendix II – Email Content Filter Categories

The following table is provided as a reference to highlight the categories of email content that are quarantined by East Ayrshire Council. The Council reserves the right to amend these categories without prior notice.

Category	Incoming	Outgoing	Internal
Virus Infection	✓	✓	✓
Large Attachments (> 15MB)	✓	✓	-
Worm Infection	✓	✓	✓
Profanity Filter	✓	✓	✓
Attachment Filter	✓	✓	✓
Image Filter	✓	✓	✓
Binary File Filter	✓	✓	✓
Script Filter	✓	✓	✓
Spam Filter	✓	-	-
Chain Email Filter	✓	✓	-
Phishing Filter	✓	-	-
Adult Website Link Filter	✓	-	-
Legal Disclaimer	-	✓	-

ACCEPTABLE USE POLICY
GOVERNING THE USE OF COMMUNICATION SYSTEMS

Appendix III – Telephony Charges

Rates of reimbursement to East Ayrshire Council – effective from 1st April, 2001.

Telephone & Fax	3p per minute for external call

Users will receive advance notification should it be necessary to alter the above rates.

ACCEPTABLE USE POLICY
GOVERNING THE USE OF COMMUNICATION SYSTEMS

Appendix IV – Acceptance & Declaration

Important: please print and complete both sections below to state that you have read, understood and agree to comply with this East Ayrshire Council policy.

……

I have read, understood and will comply with the terms set out within the Acceptable Use Policy Governing the Use of Communication Systems

Name:

Department:

Username * :

Date:

Signature:

Once completed in full, please return to your line manager / supervisor / head teacher.

……

I have read, understood and will comply with the terms set out within the Acceptable Use Policy Governing the Use of Communication Systems

Name:

Department:

Date:

Signature:

Please tear off this section and keep safe for your own records.

……

*** - this is the name that you use to log in, typically in the format "MACDONALDR4", "SMITHC" etc**