RHONDDA CYNON TAF COUNTY BOROUGH COUNCIL

INTERNET & EMAIL ACCEPTABLE USE POLICY

Version 1.2

Revised and effective from 28 August 2009

STRONG HERITAGE | STRONG FUTURE
RHONDDA CYNON TAF
TREFTADAETH GADARN | DYFODOL SICR

Document Control

Organisation	ICT Services
Title	Internet & Email AUP
Author	Tim Jones
Filename	\\adrctcictnas2\GCSX\GCSx-Project\Policies and Procedure\Policies and Procedures - Drafts Awaiting Signoff\Internet & Email AUP
Owner	Head of ICT
Subject	Internet & Email Acceptable Use
Protective Marking	Unclassified
Review date	The ICT Strategic Steering Group will formally review the Information Security Policy annually

Revision History

Revision Date	Revisor	Previous Version	Description of Revision
20/02/09	ICT SMT	1.0.	Final Document
11/09/09	ICT SMT	1.1	Amendments to reflect GCSX Use
16/09/09	C Doyle	1.2	Minor Amendments

Document Approvals

This document requires the following approvals:

Sponsor Approval	Name	Date
GCSX Project Team	Marc Crumbie (Internal Audit) Bethan Davies (HR) Deb Hughes (HR) Phil Derham (Finance)	28/08/09
ICT SMT	Elaine Pritchard John Harries Leigh Gripton	28/08/09
Head of ICT	Tim Jones	28/08/09

Document Distribution

This document will be distributed to:

Name	Job Title	Email Address
All employees, members, contractors & third party suppliers		

INTERNET & EMAIL ACCEPTABLE USE POLICY

CONTENTS

Page

1 Purpose of Internet & Email Acceptable Use Policy

1.1 The purpose of this document is to set out the Council's policy on the access and acceptable use of its Internet and Email facilities.

1.2 The Council considers the Internet to be a valuable asset that, if used correctly, can help Council staff do their job more effectively. Therefore it is Council policy to promote its proper and efficient use.

1.3 Conditions of use (including legal and regulatory matters) are detailed later in this policy but the overall purpose of these conditions is to: -

- protect the Council and its staff from legal action, either civil or criminal;
- protect the Council and its partners from embarrassment and public allegation;
- promote efficient and safe use of the Council's Internet and Email facilities; and
- avoid dispute between staff, the Council and members of the public.

1.4 The ICT Strategic Steering Group will review this Internet & Email Acceptable Use Policy every six months and re-issue it annually, drawing attention to any changes that may have been made.

2 Scope of Policy

2.1 This policy defines what the Council considers as acceptable use of its Internet and Email facilities and sets out rules and guidelines for the access and use of these facilities.

2.2 This policy applies to the use of Internet and/or Email access provided by the Council and is applicable to all members of the Council, including elected members, staff, contractors, consultants, visitors, authorised third party users and any other authorised users who access these Council Information Systems from network connected sites or remote locations.

2.3 It applies whenever they are logged on under their Rhondda Cynon Taf provided Userid and whether they are accessing the system directly via the Council's network, using a home Internet connection, an Internet café, an external Web-based Email system, a mobile phone, or any other method used where a user logs on under this Userid.

2.4 All communications sent, received or created within Council systems, together with any information stored on Council systems, are the property of the Council and as such cannot be considered as private and may be checked in accordance with the law.

2.5 All users must agree to read, understand and comply with the terms and conditions of this policy.

3 Management Policy

3.1 The Council reserves the right to examine any personal files stored on the Council's systems, this includes the contents of any files, Email or other electronic communications sent to the user. Council systems are primarily for the storage of work related material.

3.2 The ICT Service will produce reports monthly, detailing the Internet pages users have accessed and these can be provided to Service Directors \ Head of Service for review for both statistical purposes and to ensure compliance with this policy.

3.3 The Council reserves the right to monitor, access and review any individuals use of Council Computer equipment, systems and facilities covered by this policy (and related policies e.g. Councils Information Security Policy) without the additional consent being required from any employee. Monitoring will be undertaken for the purpose of business operations, audit and security or where there is reason to believe that a breach of security or a breach of policy has occurred.

4 Conditions of Internet & Email Use

4.1 Users should primarily use the Council's Internet and Email facilities for business, team building and career development activities.

Reasonable personal use is acceptable provided it :

- is undertaken in an employees own personal time and outside of core working hours or members own personal time and
- does not interfere with the performance of your official duties;
- does not take a priority over your work responsibilities;
- does not incur expense on the Council
- does not have a negative impact on the Council in any way, nor damage its reputation.

4.2 In accordance with the Council's Information Security Policy http://rctinform/content.aspx?dDocName=014412&xNodeID=5225 all users are issued with a permanent logon Userid and initial password, which they are compelled to change at least every 60 days, this allows a user certain permissions, e.g. access to the Internet and Email facilities and access to specific drives and applications.

4.3 Users are responsible for their individual accounts and as such they should take all reasonable precautions to prevent others from being able to use their account.

4.4 Personal passwords must not be written down, nor physically or electronically stored by the user.

4.5 Users must not use anyone else's password and must not directly / indirectly divulge their passwords or those of any groups that they belong to.

4.6 Do not send an ICT System or account information by Email; this includes user accounts, passwords, internal network configurations, addresses or system names. This information is confidential.

4.7 Users must check their Emails frequently; any that need to be kept should be saved in a relevant folder or on a shared drive, while those that are no longer required should be deleted.

4.8 When downloading electronic files, users must follow the computer virus protection procedures as set on your Council computer, helping to avoid the inadvertent spread of computer viruses. ICT staff will update these periodically.

4.9 Computer viruses are a type of software that can be transferred between programs or computers without the knowledge of the user, they contain instructions as to when to activate and what to do, e.g. displaying annoying messages, deleting files or infecting other programs. Many do no lasting damage but some can cause serious problems for the Council and they all constituent a breach of security.

4.10 If you suspect you have been the victim of a computer virus, or become aware of the presence of a computer virus - this includes any verbal communication you may have received from an external body - you should not under any circumstance send or forward any further Emails to any colleagues. Contact the ICT Service Desk by telephone immediately in such circumstances.

4.11 If you are informed of the presence of a hoax virus, do not make colleagues aware by any electronic means, as by doing so you may inadvertently spread the virus. Contact the ICT Service Desk by telephone immediately in such circumstances.

4.12 If users mistakenly access inappropriate information, they must immediately advise their Line Manager and report the incident to the ICT Service Desk. This will protect them against any claim that they have intentionally violated this policy.

4.13 Users must promptly disclose to the ICT Service Desk any messages or images they receive that are inappropriate or make them feel uncomfortable. The ICT Service Desk will advise on what action to take.

4.14 Users may not use the Internet & Email at anytime for example for:

- Political lobbying i.e. the process of making a concerted effort designed to achieve a political result that is against Council policy or goals. This could then in turn be harmful or cause issue for the council.

- Engaging in any illegal activity.

- Accessing material that is profane or obscene (pornography), that incites illegal acts, violence or discrimination towards other people (hate literature).

- Accessing web sites, bloggs or chat rooms that are offensive, unsuitable or inappropriate to the workplace

- When sending confidential information to external bodies, unless authenticity is established and there is adequate security in place for such transactions, first obtain approval from your Line Manager to ensure that financial and contractual rules are followed appropriately. (To avoid confusion, confidential information covers items such as employee data, customer information and financial information).

- Online gambling.

- Playing of online games.

- Engaging in inappropriate language, designated as: obscene, profane, lewd, vulgar, rude, inflammatory, threatening, or disrespectful. This applies to any public or private messages, images, audio and to any material posted on web pages.

- Posting information/material that could cause damage or a danger of disruption to Council business.

- Engaging in personal attacks, including prejudicial or discriminatory to other people.

- Attempting to gain unauthorised access to the Internet or go beyond their authorised access. This includes attempting to log in through another person's account or accessing another person's files. Sending Emails purporting to come from some other person, whether or not that person is an employee of the Council.

- Making deliberate attempts to disrupt the computer system or destroy data by spreading computer viruses or by any other means. These actions are illegal.

- Harassing another person. Harassment is defined as acting in a manner that distresses or annoys another person. If users are told by another person to stop sending them messages, they must stop. Further guidance on harassment is available through the Council’s harassment, racial harassment and sexual harassment policies.

- Knowingly or recklessly posting false or defamatory information about a person or organisation.

- Posting, forwarding or replying to chain letters or engaging in "spamming". (Spamming is the word used to describe the sending of annoying or unnecessary messages to a large number of people).

- In order to maintain system resources, users must not download large files unless absolutely necessary. If it is necessary, they should download the file at a time when the system is not being heavily used and immediately remove the file from the system on finishing with it. If you are expecting an Email attachment, which you anticipate will be larger than normal, contact the ICT Service Desk for advice.

- The downloading of applications, operating system upgrades and other programme files is strictly prohibited (ICT staff excepted), unless they are available on the Intranet or the Council's website.

- **Those Council Officers who may be required to undertake any of the prohibited actions set out in 4.14 (either as part of the Council's monitoring regime or in relation to their official duties), are required to seek prior written authorisation from their Head of Service and the Head of ICT).**

Personal Use of Internet and Email

Acceptable personal use

4.15 Users may use the Council's Internet and Email facilities for reasonable personal use. Reasonable use of the Council's Internet and Email facilities is only permitted outside of normal core time working hours and is only acceptable during an employees personal time. i.e. before or after work, during lunchtime and is subject to staff clocking\signing out. Users should note that this is a privilege and not a right, which can be removed at any time.

For additional clarity the Statement of Policy on Flexible Working Hours can be located at: http://rctinform/content.aspx?dDocName=014412&xNodeID=5073

4.16 Subject to this policy personal use could include but is not solely restricted to areas such as Online Banking, Shopping, Entertainment, Leisure Activities or bookings, Personal Research and Web Based Email services e.g. MSN and Hotmail. All such use is carried out at users' own risk and the Council does not accept responsibility or liability for loss caused as a result of use of the Internet.

4.17 The conditions of use set out in the **Section: 4.14** apply equally to the personal use of the Council's Internet and Email facilities.

4.18 Users are reminded that all Internet and Email activity is monitored and traceable at all times, therefore remember that when you are accessing the Internet and Email facilities for personal or business use, any activity will be logged via Council ICT systems.

4.19 The Council appreciates that certain private Emails may be sent to and from your work Email account but this must be kept to a minimum.

4.20 Use of GCSx Email

- All Council employees that require access to GCSx email must read, understand and sign the GCSx Acceptable Usage Policy and Personal Commitment Statement.
- All emails sent via the Government Connect Secure Extranet (GCSx) must be of the format "@RCTCBC.gcsx.gov.uk".
- Any emails containing PROTECT or RESTRICTED information must be sent from a GCSx email account
- 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 into one of 6 classifications. The way the document is handled, published, moved and stored will be dependant on this scheme.

The classifications are:

- UNCLASSIFIED
- PROTECT.
- RESTRICTED.
- CONFIDENTIAL.
- SECRET.
- TOP SECRET.

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

All external email contains will contain the following disclaimer notice:-

“This transmission is intended for the named addressee(s) only and may contain sensitive or protectively marked material up to RESTRICTED and should be handled accordingly. Unless you are the named addressee (or authorised to receive it for the addressee) you may not copy or use it, or disclose it to anyone else. If you have received this transmission in error please notify the sender immediately. All traffic including GCSx may be subject to recording and/or monitoring in accordance with relevant legislation.”

For the full disclaimer please access http://www.rctcbc.gov.uk/disclaimer “

5 Monitoring and Enforcement

5.1 All communications and stored information sent, received, created or contained within the Councils ICT systems are the property of the Council and accordingly should not be considered as private and may be checked in accordance with the law. The Council reserves the right to bypass any security setting that an employee may make, in order to protect the Council’s interest.

5.2 Details of all Internet and Email activities leave an ‘electronic footprint’ on both personal computers and the Internet servers. The ICT Service will produce monthly reports detailing usage activity and these will be provided to Service Directors \ Heads of Service for review, for both statistical purposes and to ensure compliance with this policy.

5.3 **The ICT Service may undertake Internet & Email monitoring periodically and without notice for the following purposes:**

- To help maintain compliance with regulatory or self-regulatory practices.

- To provide local Service management with usage statistics and reports to assist with the day-to-day management of their services. (It is the responsibility of each local Service manager to assess the provided reports).

- To support local service managers in the interpretation of usage statistics and reports. It is the responsibility of each local manager to use the provided reports to monitor the usage of their staff and enforce the usage policy.

- To establish facts and protect the interests of the Council and employees.

- To prevent unauthorised use of the Council's ICT systems.

- To prevent inappropriate/offensive media from entering the workplace.

- To assist with any investigation whether internal or by externally authorised investigating authorities (e.g. Police, Internal or External Audit).

- To comply with the Council's access to information obligations under the Data Protection Act 1998 and the Freedom of Information Act 2000 or any statutory modification under such acts.

5.4 The Council reserves the right to make and keep copies of all information, including, but not limited to Emails and data documenting the use of the Internet and Email systems for the purposes set out above.

5.5 The Council reserves the right to place restrictions on the use of Internet and Email accounts at any time.

6 Consequences of Breach to Policy

6.1 Any breach of this and related policies may warrant further investigation that may lead to the Council's disciplinary procedures being invoked and in certain circumstances, may necessitate the involvement of the Police.

6.2 The Council will co-operate fully with any Audit or Police investigation. If the investigation demonstrates that material that is accessed is offensive, e.g. pornographic, advocate's illegal acts, violence or discrimination to other people, this will be considered gross misconduct and appropriate disciplinary procedures will be followed, possibly resulting in dismissal.

7 Reporting Security Events (Breach of Controls)

7.1 Any employee or computer user of the Council who considers that this policy has not been or is not being followed by any user in respect of Email or Internet usage, the results of which could be damaging to other staff, users, the Council, or illegal in any way, are encouraged to raise the matter with their Line Manager, or Head of Service and follow the Information Security Incident Management Policy.

7.1 If any potential breach of these rules comes to the attention of Service Managers, management should in consultation with Human Resources instruct ICT Services and or Internal Audit to investigate further. It will be for Service Managers in consultation with Human Resources to consider whether disciplinary action in accordance with the Councils disciplinary procedures is appropriate.

7.2 All staff or agents of the Council will be encouraged to report any security event, actual or potential, without fear of recrimination. Every effort will be made to learn lessons from security events in order that preventative controls may be put in place for the future.

7.3 Where an employee or computer user of the Council inadvertently makes a genuine mistake or the unexpected occurs it should be reported to their Line Manager or the ICT Service Desk.

8 Compliance with Legislation and Regulation

8.1 Users should note that an Email has the same significance and legal implications as a signed letter. Furthermore users should never send ‘off the record’ Emails – nothing is ‘off the record’ where the law requires disclosure of information.

8.2 Messages sent via the Email system can give rise to legal action against the Council. Claims of defamation, breach of confidentiality or contract could arise from the misuse of the system.

8.3 Emails must never contain what could be considered as a defamatory statement, i.e. one that may possibly damage the reputation of another individual or company. Remember that damaging Emails may have to be disclosed in litigation or in investigations by other councils or organisations. Users are also reminded that messages can be disclosed in any legal action commenced against the Council relevant to the issues set out in the Email.

8.4 Do not transmit / receive graphical images or scanned signatures either as an attachment or embedded as a signature to Email. These graphical files could easily be copied and applied fraudulently to other documents e.g. faxes or electronic letterheads.

8.5 Users will respect the rights of copyright owners. Copyright infringement occurs when items protected by copyright are inappropriately reproduced. Where items contain conditions regarding their use, these should be followed. Users should request permission from the copyright owner if they are unsure as to whether or not such items can be used.

8.6 Users should be aware of UK and international laws that govern the use of Emails. These include any statutory modifications or amendments but are not limited to:

- Copyright
- Libel and Defamation
- Public Records Acts 1958 and 1967
- Data Protection Act 1998
- Human Rights Act 1998
- Freedom of Information Act 2000
- Regulation of Investigatory Powers Act 2000
- Electronic Commerce (EC Directive) Regulations 2002

9 General Email Responsibilities

9.1 Email Housekeeping

- Good practice is that you should save the Email in the relevant folder on a personal or preferably a team shared drive. This brings together all documents relevant to a theme or activity and will make it easier for you or your colleagues to search for work-related Emails and related documents.

- Add to or amend the original subject line if this helps with filing. Delete all Emails that do not need to be saved as soon as possible.

- The Council has set a limit on the size of mailboxes, which includes Inbox,
Sent Items and Deleted Items, and once the limit is reached an employee will not be able to send or receive Emails. It is the responsibility of each individual to

manage his / her mailbox. The owner of the inbox will receive an automated reminder as that limit is approached and unless action is taken to reduce its size, no further Emails will be accepted or sent for that person until action is taken. Users should regularly carry out 'housekeeping' of their mailbox.

- Read and delete Emails regularly. Keep your 'Inbox', and 'Sent' folder contents to a minimum. Regularly delete 'Deleted items' and associated sub-folders.

- Create folders for Email categories, people, services, sections etc.

- Create archive files on PC hard disk to enable transfer of old Email messages from the central server to your PC (contact ICT Service Desk for help and guidance with this).

9.2 Email Etiquette

- Use Email facilities with a sense of professional conduct.

  Avoid typing everything in CAPITALS.

  THIS CAN BE CONSIDERED TO BE THE EQUIVALENT OF SHOUTING!

  Similarly, be sparing in the use of UNDERLINE and **BOLD**.

- Good practice is that all Emails should be formatted as Arial 12, as per the clear print guidelines.

- Do not send messages with a blank subject line. The recipient has no indication as to whether the message is of value and will have to amend the field to give their own version of the subject if they wish to file it sensibly.

- Do not send large file attachments unless they are expected. These could fill the recipient's mailbox and they may not be able to receive further Email until they have deleted yours. In a few cases it could mean that your Email is returned automatically to you without reaching the intended recipient.

- In many organisations, attachments that are not of a major recognised file type are not opened. As they can be a common way of reproducing viruses, they may be rejected either automatically or by recipients obeying their organisation's rules (• doc, .xls, .mdb, and .pdf file types are usually acceptable -these are from Microsoft Word, Excel, Access and Adobe Acrobat respectively).

- If you require to send a file type other than those listed above, you may wish to contact the intended recipient in the first instance to ensure their system can receive it (if external to the Council) or contact the ICT Service Desk for further advice.

- If you accidentally receive someone else's Email, redirect it; if that is difficult, return it to sender. If the message is internal, consider whether adjacent entries in the address book are causing confusion.

- Do not send Emails addressed to “Everyone”, i.e. Global, where you require this facility, contact the Council’s internal communications officer and - or the ICT Service Desk to discuss utilising the Council intranet.

- Use the “Out of Office Assistant” if you know you will not be able to access your Email system for a period of time. Good practice is to explain when you will be returning to work and whom the person can contact in your absence to deal with queries. Remember the Out of Office Assistant can be read by external organisations, so ensure your message is professional in its content.

- Do not send non-work related Emails to large numbers of people who have not agreed to receive them, even if the contents may appear to be of interest. This is sometimes known as spam, bulk, chain or junk mail.

- The ICT Service provides central systems to block unwanted or spam Email. These automated systems provide a high level of protection, however these systems are not 100% fail safe and it maybe possible for spam mail to be received. Under this circumstance it is the responsibility of staff that receive them to deal with them, in consultation with the ICT Service Desk.

If spam Emails are received, consider: Is it from a known person or company? Was the Email requested by providing your details on a website or on a paper form? Does it contain useful information relevant to your work or the Council’s business?

Post consideration: Read, and delete or save as necessary

----------End of policy document----------