



Acceptable Use Policy

DQ Status	Live	Policy		
DQ Content Authority	Controller IT (Keith Little)			
Contact(s) for Help	Julia Harris (Head of Information Security)			
Description	<p>Intended Audience: Applies to employees and contractors working for the BBC and any subsidiaries.</p> <p>Use: This policy describes acceptable (and unacceptable) use for access to BBC Electronic Networks and computers and must be read and followed by all Authorised Users.</p> <p>Internet, Intranet and e-mail access provided by the BBC is intended for BBC business use, but limited access for personal use is allowed. The AUP includes references to computer security, 'netiquette' use and misuse of BBC resources.</p>			
DQ Reference	Version	Date	Last Reviewed	Next Review Due
email_07	02.00	29/10/2004	Sept 2004	Sept 2005
Key Words	Email, internet, policies for staff			
DQ Location	Internal: http://guidelines.gateway.bbc.co.uk/dq/email/acceptable_use.shtml External: http://www.bbc.co.uk/guidelines/dq/contents/email.shtml			

BBC Acceptable Use Policy (AUP)

This is a policy that applies to employees, temps, freelancers and contractors working for the BBC and any subsidiaries or service providers under contract and is issued under the authority of the Head of IT and Data Assurance. It describes acceptable (and unacceptable) use of BBC Electronic Networks and must be read and followed by all Authorised Users.

Information Processing Equipment, Internet, Intranet and e-mail access provided by the BBC is intended for BBC business use, but limited access for Personal Use is allowed. The BBC encourages the use of the Internet, Instant Messenger, Live Communication Server, Instant Relay Chat (IRC), BBC Talker, Intranet (Gateway) and e-mail, because they make communication and research more efficient and effective. Use of the BBC's time, facilities, equipment or supplies for an employee's or contractors' private business is prohibited. This AUP has been created to ensure that all employees and contractors understand the basis on which access is allowed.

This AUP includes references to information security, 'netiquette' use and misuse of BBC Electronic Networks and Information Processing Equipment.

Where there is a requirement to attach to BBC Electronic Networks with high levels of access, from insecure or dangerous situations (i.e. war or disaster zones), Authorised Users will be requested to sign acceptance of this policy and send to the BBC Information Security Team, MC4 B3, Media Centre.

Any enquiries should be made to the BBC Information Security Team (ism@bbc.co.uk).

AUP Index

Definitions
Computers
Electronic Networks
BBC Information Processing Equipment
Data
Download
BBC Intranet
Internet
Authorised Users
Overview
Statement of Use
Compliance
Expectation of Privacy
Conditions of Use
Authorised Use
Personal Use
Prohibited Use
Examples
Network Security
BBC Email
Remote Access - Home Equipment
Remote Access - BBC Equipment
Remote Access - Cyber Caf��s
Network unfriendly activity
Copyright
Unacceptable Use - Examples
Failure to Comply
Enforcement /Actions to be Taken
Enforcement Guidance to Managers
References
Related References

[^top](#)

Definitions

Information Processing Equipment

Information processing equipment includes, but is not necessarily limited to, a personal computer, laptop, wireless communication device, personal digital assistant, hub, server, communications equipment, or playout device that may be connected, once authorised, to the BBC Electronic Network, or operated on a standalone basis that can process and/or store signals or information.

[^top](#)

Electronic Network

An electronic network is a group of Information Processing Equipment that can communicate with/via each other. Electronic Networks include the following:

- The public Internet;
- networks internal to the BBC;
- contracted service provider networks; and
- public and private networks external to BBC.

[^top](#)

[^top](#)

Data

Confidential data is information that requires a high level of protection due to the risk and/or magnitude of loss or harm to the BBC that could result from disclosure, alteration or destruction of the data.

Sensitive data is information that requires some level of protection because its unauthorised disclosure, alteration, or destruction will cause perceivable damage to the BBC.

[^top](#)

Download

Downloading is the act of transferring data from remote Information Processing Equipment to local Information Processing Equipment and optionally storing it on local Information Processing Equipment.

[^top](#)

BBC Intranet

The BBC Intranet is the BBC internal Electronic Network that uses a common communication protocol to enable BBC Information Processing Equipment of all kinds to directly and transparently communicate and share services. The BBC Intranet web service provided that runs on this network is referred to as “Gateway”.

[^top](#)

Internet

The Internet is a global information Electronic Network consisting of national, regional and private Electronic Networks that use a common communication protocol and cooperate to provide their users with a common interface.

[^top](#)

Authorised User

An Authorised User is:

A BBC employee; or

A temporary BBC staff member, a member of a BBC service provider’s staff, a freelancer, a contractor or other person not directly employed by the BBC who has been authorised by or on behalf of the BBC to use BBC Information Processing Equipment.

[^top](#)

Overview

Statement of Use

This AUP provides direction to Authorised Users on the use of BBC Information Processing Equipment.

Uses of BBC Information Processing Equipment are separated into the following categories:

Authorised Use;

Personal Use; and

Prohibited Use.

Authorised Users shall only use BBC Information Processing Equipment for Authorised Use and Personal Use. Authorised Users shall not use BBC Information Processing Equipment for any Prohibited Use. The Failure to Comply paragraph outlines actions that may be taken in the event of Prohibited Use.

[^top](#)

Compliance

It is the responsibility of each Authorised User to take all reasonable steps to ensure compliance with the conditions set out in this AUP document, and to ensure that Prohibited Use of BBC Information Processing Equipment does not occur.

It is preferable for misuse to be prevented by a combination of technical solutions and responsible attitudes to the use of BBC Information Processing Equipment on the part of users.

Where violation of these conditions is illegal or unlawful, or results in loss, alteration or disclosure of Data or BBC Information Processing Equipment, the matter may be referred for legal action.

[^top](#)

Expectation of Privacy

Users should assume that electronic communications across the Internet cannot be considered private or secure and should consider the sending of confidential, sensitive or personal information (sensitive and personal information are as defined by the Data Protection Act 1998) by other means.

BBC Information Processing Equipment are subject to tracking (using logging and audit facilities) for purposes of ensuring compliance with BBC policies, system administration, maintenance and security as part of the normal course of BBC business practice. Monitoring is permitted for the purposes of a specific investigation and detailed under the BBC policy on the Regulation of Investigatory Powers Act 2000. The Data Protection Act 1998 also contains monitoring clauses.

[^top](#)

Conditions of Use

Authorised Use

Authorised Use is any use of BBC Information Processing Equipment that is necessary to carry out official duties and functions in furtherance of BBC business, goals and objectives, and includes:

use of BBC provided Information Processing Equipment in any BBC premises;

use of BBC provided portable Information Processing Equipment, including synchronisation of such devices;

communicating with colleagues, the public, and the private sector; and

conducting research for departmental purposes.

Authorised Users should note that this policy does not restrict or modify the mandate or legitimate activities of any organisation that uses BBC Information Processing Equipment as a means to conduct BBC business operations.

[^top](#)

Personal Use

Personal Use is any use of BBC Information Processing Equipment that, while not necessary to carry out official duties in furtherance of BBC goals and objectives, is for:

- communicating with family, friends and other persons for other than official purposes;
- accessing news and other Electronic Network information sources that are not prohibited;
- conducting routine personal banking transactions;
- shopping for, and purchasing of, personal and family items;

Personal Use of BBC Information Processing Equipment may only be of a reasonable duration and frequency and shall not interfere with the performance of the official duties and functions of an Authorised User or any other person.

Personal Use may be permitted at the discretion of the Authorised User's manager or supervisor. Personal Use of the Internet is not considered part of an Authorised User's paid work time.

Heads of Technology, Line Managers and Supervisors at all levels may restrict or prohibit any Personal Use of BBC Information Processing Equipment if:

- the use threatens the capability or integrity of BBC Information Processing Equipment; or
- the restriction or prohibition is otherwise necessary for operational or administrative reasons.

[^top](#)

Prohibited Use

Prohibited use is any use of BBC Information Processing Equipment that is not:

an Authorised Use; or

a Personal Use.

Prohibited uses of BBC Information Processing Equipment include, but are not necessarily limited to:

any Personal Use that exceeds a reasonable duration or frequency;

any Personal Use that interferes with the performance of the official duties and functions of an Authorised User or any other person;

any use that would result in personal profit, e.g., electronic gaming;

any use of peer to peer/content sharing network software (e.g. Kazaa or Napster) to transmit or access material into/out of the BBC;

any use which involves a personal business venture (except where the personal business venture is contracted by the BBC, and the use is for preparation of paperwork (e.g. invoices or timesheets) for the BBC);

accessing or distributing any material whose main focus is pornography, nudity, sexual acts or the incitement of hatred;

downloading or use of unauthorised programs. BBC Information Processing Equipment must not be modified in its setup or have additional software installed unless so directed by BBC support staff. You may not copy, change, or transfer any software provided by the BBC without permission. Usage of unlicensed software is illegal, and may lead to the prosecution of the BBC. Usage of unauthorised software greatly increases the risk of software conflicts, viruses, and other incompatibilities, which could result in permanent damage and loss of data;

any Personal Use restricted or prohibited under this AUP by a Line manager or Supervisor or Head of Technology;

any use contrary to any order, instruction or other BBC policy issued by or on behalf of the BBC;

- any use that would bring discredit upon the BBC;
- any use contrary to the *Criminal and Statutory Law*,
Copyright Law, any other European or Government
statute or regulation, or law, including any non-criminal
statute or regulation;
- any use that has or could reasonably have caused harm to
others;
- any use that is an intentional action that would jeopardise
the integrity of BBC Information Processing Equipment
or bring the BBC into disrepute;
- any use that could result in court proceedings and/or the
civil liability of an Authorised User.
- any unlawful activity.

The BBC manages Internet filtering (blocking) of individual websites or classes of websites. Requests for exceptions or authorised access to any filtered site should be directed to the Information Security Manager (ism@bbc.co.uk), or by completing the request form on the BBC Intranet site.

[^top](#)

Examples

Network Security When connecting to BBC Information Processing Equipment, Authorised Users must consider and conform with the following :-

Authentication - Authorised Users are responsible for controlling the access to their computers, properly logging on and off Electronic Networks, and not using another user's UserID. Unauthorised distribution of passwords and/or access codes is strictly prohibited. Your UserID belongs to you, and you are responsible for all actions taken with it.

Attempting to circumvent user authentication or security of any Information Processing Equipment, Electronic Network, or account (aka "cracking") is strictly prohibited. This includes, but is not limited to, accessing data not intended for the user, logging into a server or account the user is not expressly authorised to access, or probing the security of BBC servers and networks.

Impersonation/Forgery - Adding, removing, or modifying identifying network header information (aka "spoofing") in an effort to deceive or mislead or attempting to impersonate any person and/or equipment by using forged headers or other identifying information is strictly prohibited.

Equipment Attach – Adding any equipment to the BBC Electronic Network must follow the process laid down by the End Systems Attachment Policy held on the Delivering Quality web site - <http://guidelines.gateway.bbc.co.uk/dq/index.shtml>

[^top](#)

BBC Email

Authorised Users must consider and conform with the following for e-mail activities:-

E-mail communication must reflect professional and respectful business correspondence standards and must not be libellous or use abusive language.

Each Authorised User is responsible for the content of all text, audio or images that they place on or send over the Internet, Intranet or e-mail. No e-mail or other electronic communications may be sent which hides the identity of the sender or represents the sender as someone else. All messages communicated on the Internet, Intranet or e-mail system should contain the Authorised User's name. An Authorised User may be a mailing list for bulk mailings to consumers, viewers, listeners etc.

[^top](#)

Remote Access - Home Equipment

When connecting to BBC Information Processing Equipment using equipment that is under the control of the Authorised User but not owned by the BBC, the following must be considered :-

The equipment must be regularly checked to ensure it is secure from viruses, Trojans and other malicious software that could be used (knowingly or unknowingly by the equipment's owner) to attack BBC Information Processing Equipment. Any electronic materials to be brought into contact with the BBC Information Processing Equipment must also be checked.

Antivirus (AV) software must be used and regularly updated as soon as new patches and virus signature's are released, to ensure the security and integrity of the equipment. AV software is available as freeware or can be purchased for a moderate fee.

Firewalls must be used to block 'attacks' on personal Information Processing Equipment. This is especially recommended where the equipment is connected to a broadband or 'always on' service. Firewall software is available as freeware or can be purchased for a moderate fee.

Trojan, **Adware and Spyware Scanners should** also be used to ensure the **equipment** is not infected with unwanted applications **which** might **broadcast** information unknowingly to third parties, **and/or might** allow the **equipment** to be remotely controlled by third parties Trojan, Adware and Spyware scanner software is available as freeware or can be purchased for a moderate fee.

If the equipment is running Windows operating systems, the automatic update options should be activated within Windows update, to ensure that the system is kept current with available security patches. If running other operating systems, reference the relevant site to ensure they are correctly patched.

Other household members must not be granted access to the equipment whilst it is connected to the BBC Electronic Network.

Further guidance and technical support is available from the BBC Helpdesk on xtn 0226333.

[^top](#)

Remote Access - BBC Equipment

When BBC Information Processing Equipment, under the control of an Authorised User, connects to the BBC Electronic Network via non BBC Electronic Networks, the subsequent clauses must be followed :-

The Authorised User should be mindful of the environment in which their Information Processing Equipment is being used. Care should be taken that third parties are not snooping, overlooking the Information Processing Equipment's screen or are in a position to read sensitive information from the screen.

The Authorised User must ensure that BBC antivirus and other BBC initiated downloads are accepted wherever practicable in order to keep the Information Processing Equipment up to date and maintain the security of the BBC. Persistent failure to do so will result in restricted access to BBC Information Processing Equipment until such updates have been successfully applied.

The Authorised User may not modify any components specific to the security of the Information Processing Equipment – specifically machine identification information, the VPN, Antivirus or Firewall configurations, unless so directed by BBC support staff.

The Authorised User must take responsibility for the reasonable care and protection of BBC Information Processing Equipment while they are in their possession. Laptops are NEVER to be left unattended unless they are properly secured, unless it is in the Authorised User's house, or locked in a hotel safe.

Authorised Users are responsible for reporting loss, damage, and other problems to the BBC as soon as possible.

Authorised Users must ensure that no unauthorised users can use the Information Processing Equipment whilst it is connected to the BBC's Electronic Network.

[^top](#)

Remote Access - Cyber Cafés - When connecting to the BBC Electronic Network using Information Processing Equipment that is not under the control of the Authorised User and not owned by the BBC or the Authorised User, the subsequent clauses must be followed :-

When browsing or surfing to any BBC email or Intranet information, copies of files or pages viewed should be deleted and not left on the Information Processing Equipment being used.

When printing any BBC information, temporary copies of files or pages printed should be deleted and not left on the Information Processing Equipment being used. For help on performing this task, ring the helpdesk on 020 8752 6333.

When viewing any BBC email or Intranet information in a public place, ensure that people are not obviously snooping or reading private information proprietary to the BBC

[^top](#)

Network unfriendly activity

Any activities which adversely affect the ability of other people and systems to use the BBC Information Processing Equipment are prohibited. This includes "denial of service" attacks against any servers, network equipment or individual user.

Use of any program/script/command, or sending messages of any kind, designed to interfere with an Authorised User's session, by any means, locally or by the Internet.

Unauthorised sending of unsolicited commercial e-mail. Using any bulk e-mail facility or Website address to distribute unsolicited commercial e-mail.

Unauthorised sending large volumes of unsolicited e-mail (aka "mail bombing").

[^top](#)

Copyright

Users must honour copyright laws regarding protected commercial software, music or any intellectual property. Duplicating, transmitting, or using software not in compliance with software license agreements is considered copyright infringement. Authorised Users shall not make copies of software, music or literature in violation of copyright laws without the full legal right to do so. Unauthorised use of copyrighted materials or another person's original writings is considered copyright infringement. Copyrighted materials belonging to others may not be transmitted by staff members on the Internet without permission. Users may download copyright material from the Internet, but its use must be strictly within the agreement as posted by the author or current copyright law. Copyrighted agency information used on web sites must be clearly labelled as such.

[^top](#)

Unacceptable Use BBC Information Processing Equipment may not be used for any of the following:
- Examples

the creation or transmission (other than for properly supervised and lawful research purposes, with the express permission of the BBC) 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;

the creation or transmission of material which is designed or likely to cause provocation, inconvenience or needless anxiety;

the creation or transmission of defamatory material;

the transmission of material that infringes the copyright of another person or organisation;

the transmission of unsolicited material, except where that material is part of a service to which the recipient has chosen to subscribe;

deliberate unauthorised access to facilities or services accessible via BBC Information Processing Equipment;

deliberate activities with any of the following characteristics:

wasting BBC staff effort or resources, including time on end systems accessible via BBC Information Processing Equipment and the effort of staff involved in the support of those systems;

corrupting or destroying other users' data;

violating the privacy of other users;

disrupting the work of other users;

in a way that denies service to other users (for example, deliberate or reckless overloading of access links or of switching equipment);

continuing to use an item of networking software or hardware after the BBC has requested that use cease because it is causing disruption to the correct functioning of BBC Information Processing Equipment;

other misuse of BBC Information Processing Equipment or resources, such as the introduction of "viruses";

knowingly transferring or allowing to be transferred to, from or within the BBC, textual or graphical material commonly considered child pornography;

any purpose which is illegal, or is against statutory law or BBC

policy;

for-profit and non-profit business activities including activities for service organisations not related to the job;

excessive use for private, recreational or personal activities;

gambling;

raising funds for political candidates or issues;

personal advertisements e.g. for house/flatshare, cars etc, except in authorised places such as talk.gateway and Ariel;

promoting political candidates in any way;

promoting personal political issues;

gathering information for furtherance of a crime;

circulating chain letters or pyramid letters;

downloading, installing, or running security programs or utilities which might reveal weaknesses in the security of the BBC Information Processing Equipment unless a job specifically requires it;

attempting to modify, install or remove Information Processing Equipment, software, or peripherals without proper authorisation. This includes installing any non-work related software on BBC-owned equipment;

accessing Information Processing Equipment, software, data information, or networks without proper authorisation, regardless of whether the Information Processing Equipment, software, data, information, or network in question is owned by the BBC. (This means, if you use the Electronic Networks to which the BBC has access or the Information Processing Equipment at other sites connected to those networks for which you do not have authorisation, the BBC will consider this matter an abuse of your access privileges, and violation of this policy.);

circumventing or attempting to circumvent logon procedures, and security regulations, or exceeding the system's capacity limits by downloading excessive materials;

the use of Information Processing Equipment facilities, UserIDs, or data for purposes other than those for which they are intended or authorised;

breaking into another user's e-mailbox, or unauthorised personnel reading someone else's e-mail without permission;

sending fraudulent electronic transmissions, including but not

limited to, statements intended to mislead the receiver which are known to be untrue, fraudulent requests for confidential information, fraudulent submission of electronic purchase requisitions or journal vouchers, or fraudulent electronic authorisation of purchase requisitions or journal vouchers;

violating any software license agreement or copyright, including copying or redistributing copyrighted software, data, or reports without proper, recorded authorisation;

taking advantage through social engineering or other methods of another user's naiveté or negligence to gain access to any UserID, data, software, or file that is not your own and for which you have not received explicit authorisation to access;

physically interfering with other users' access to the BBC's computing facilities;

encroaching on or disrupting others' use of the BBC Information Processing Equipment by creating unnecessary network traffic (for example, playing games, usage of peer to peer software or sending excessive messages); excessive use of memory, bandwidth and disk space resources; interfering with connectivity to the network; modifying system facilities, operating systems, or disk partitions without authorisation; attempting to crash or tie up a BBC Information Processing Equipment; damaging or vandalising BBC Information Processing Equipment, software, or data files);

disclosing or removing proprietary information, software, printed output or magnetic media without the explicit permission of the owner;

reading other users' data, information, files, or programs on a display screen, as printed output, or via electronic means, without the owner's explicit permission;

use of Information Processing Equipment and/or UserIDs for which there is no authorisation, or use of Information Processing Equipment and/or UserIDs for purposes outside the scope for which they have been issued.

Where the BBC Information Processing Equipment are being used to access another network, any abuse of the acceptable use policy of that network will be regarded as unacceptable use of BBC Information Processing Equipment.

[^top](#)

Failure to Comply

Enforcement /Actions to be Taken

Should the BBC discover contravention of this AUP, the BBC reserves the right to take one or more of the following courses of action:

revocation of access to BBC Information Processing Equipment, either in whole or in part. The BBC shall make written/electronic notification to the user of any temporary suspension, and the cause thereof, as soon as reasonably possible. This temporary suspension will remain in effect until the Prohibited Action(s) has ceased;

investigations which may result in

charges or prosecution being laid under the *Statutory or Criminal Law* or other European statutes or regulations;

civil liability; or

disciplinary action in line with BBC policy.

For **contractors, temps, service provider staff, freelancers and other persons** who have been authorised to use BBC Information Processing Equipment, Prohibited Use of BBC Information Processing Equipment may result in termination of contracts and/or criminal charges, depending on the circumstances.

[^top](#)

Enforcement Guidance to Managers

Managers and supervisors should consider the following circumstances as a minimum before taking any action as set out above in the *Enforcement/Actions to be Taken* paragraph in any case of prohibited use:

the nature of the prohibited use; and/or

the frequency of similar activity within the department;
and/or

the impact of the prohibited use on unit morale and
discipline; and/or

any impact the prohibited use had or may have had on the
unit's operational capabilities.

Administrative action -e.g. the withholding of access to certain BBC Information Processing Equipment or facilities may be a course of action taken by departmental managers without invoking the BBC disciplinary procedure.

Formal Disciplinary proceedings may be taken in the case of any **prohibited use** by a user, in conjunction with any necessary administrative action.

[^top](#)

References

Related References

Further information on the following related policies is available on the BBC (Gateway) Intranet site.

BBC Information Security Policy

Approved BBC IS Papers

End Systems Attach Policy

Data Protection Act

Computer Misuse Act

Copyright, Designs & Patents Act

Lawful Business Practice Regulations

Federation Against Software Theft (FAST)

[^top](#)

I agree to abide by the rules laid down in this Acceptable Use Policy.

Signed _____

Date _____

Name _____

Dept _____

Staff Number or Reference _____

Reason for usage _____

Document Control

V0.5	Draft version	Alan MacGechan
V1.0	Draft version for comment by BBC ISSG	Julia Harris
V1.1	Second Draft including comments reviewed by Information Security Team	Julia Harris
V1.2	Second Draft including ISSG comments	Julia Harris