BBC Acceptable Use Policy

DQ Status	BBC Policy
DQ Content Authority	Head of Information Security (Julia Harris)
Contact(s) for Help	Julia Harris
Description	Applies to employees and contractors working for the BBC and any subsidiaries. **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. 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.

DQ Reference	**Version**	**Date**	**Last Reviewed**
is_19_02	03.09	25/05/2008	May 2010
Who reviewed	Brian Brackenborough		
Key Words	e-mail usage, internet usage, information security, information security policy, acceptable use, disciplinary		

BBC Acceptable Use Policy

1 Introduction

This acceptable use policy (the "policy") sets out what you can and cannot do with BBC IT and related equipment. It applies to all BBC staff, contractors and anyone who accesses BBC Equipment ("BBC Users"). In this policy "BBC Equipment" means all BBC computer and telecoms systems – which includes but is not limited to the internet, intranet, email systems and telephones.

It's important for you to be able to make full use of the BBC Equipment when you are involved in BBC work. The BBC also allows limited and appropriate personal use of these resources for BBC Users. However, personal use should only ever be of a reasonable duration, capacity and frequency and should not interfere with your work.

This policy is designed to help you understand the appropriate limits on your use of BBC Equipment. The basic guide is that you shouldn't do anything using BBC Equipment that would not be appropriate in the off-line environment. This policy applies at all times, not only during working hours.

This policy should be read in conjunction with the Editorial Guidelines and the BBC Data Protection Handbook.

This policy has been drafted by BBC People, Information Policy and Compliance, Information Security and Investigation Services and will be reviewed and updated by BBC Information Security, and ratified by the Information Security Steering Group.

BBC

2 Table of Contents

3 Objectives

Compliance with this policy will ensure that:

- both individuals and the BBC are better protected from any legal action;
- email correspondence with third parties is in an appropriate format and the appropriate levels of confidentiality and security are maintained;
- the BBC's IT systems perform optimally for their intended use;
- the BBC email system is used in a way that provides a cost effective and efficient form of communication; and
- the BBC maintains high standards as set out in guidance such as the BBC Editorial Guidelines.

4 Important

It is vital that you read this policy carefully. If there is anything you do not understand, it is your responsibility to ask your manager to explain.

It is essential that you understand that if you fail to comply with this policy that you may be subject to BBC's disciplinary procedures and/ or legal proceedings. Your failure to comply may also result in legal proceedings against the BBC.

BBC's Equipment should provide all functionality you need to do your job. Should you feel you require additional functionality the BBC will have a process to enable you to resolve these issues. Please approach your ITC in the first instance. To find your ITC please use the Siemens Portal Help & Contacts link.

5 General Principles and Personal Use

- BBC's Equipment is provided for business use so that the BBC can carry out its obligations under the Charter.
- You should not use BBC Equipment in any way that is going to interfere with the proper running of the BBC, significantly distract you and/ or others from your work, interfere with the performance of your or others duties or breach the rules set out in this policy.
- Use of disk storage and network capacity for personal use must be reasonable and should not impact the BBC's ability to fulfil its business objectives.
- You understand that the BBC may monitor your use of BBC Equipment for security purposes and also to check your compliance with this policy at any time and without notifying you.
- The BBC may scan all incoming and outgoing email messages and attachments for unsuitable content.
- The BBC may decide to limit your ability to use BBC Equipment for personal use where the BBC considers this is appropriate due to possible or actual interference with BBC business. This would be decided by your line manager with input from BBC People.
- Your use of BBC Equipment is subject to all applicable laws and any illegal use will be dealt with in accordance with these laws.
- You mustn't use BBC Equipment for any business activities that are not related to your work at the BBC.

6 Internet

6.1 General Use

- You must not visit internet sites that contain pornographic, obscene, indecent, hateful or other offensive material (for example, material that contains racist terminology or nudity) except where you are expressly required to do so in the course of your work. If you're not a programme maker it's most unlikely that you will be required to access such material (and even then most programme makers won't need this access). In nearly all circumstances access to illegal content is not allowed (although please see the section below "Accessing offensive material for journalistic or research purposes").
- You must not use the BBC Equipment to participate in online gambling or multi-player online games, or for soliciting for personal gain or profit.
- You must not download software onto BBC Equipment (including any software available for free on the internet) without obtaining permission/ following the procedure at http://sbsportal.bbc.co.uk/alarms/forms/softwareevaluation.html It is important that you do not download software without permission so that the BBC can maintain the integrity of its systems and prevent unnecessary interference and downtime - see the Security Section below for details.
- Your use of social networking sites such as Facebook must not interfere with BBC work.
- The BBC reserves the right to block access to any internet site that is interfering with the operation of normal BBC business (e.g. where the amount of traffic is interfering with access to other work-related material on the internet).
- Remember that a cookie may be placed on your computer after you visit a website which will be traceable back to the BBC.
- You must not commit the BBC to any form of contract through the internet.
- You are responsible for the security of your computer terminal (whether desktop or laptop) and must not allow the terminal to be used by an unauthorised person.
- If you leave your terminal unattended for any time you must lock it by pressing Ctrl + Alt + Del and selecting 'Lock Workstation' or you should ensure that you log off. This is to help prevent unauthorised users accessing the BBC system in your absence.

6.2 Providing content

- You must not post indecent, offensive or defamatory (including libellous or slanderous) material on the internet including when blogging or in message rooms. When posting material, it is your responsibility to comply with all applicable laws – such as copyright and sexual harassment laws. Please see below for an explanation of what constitutes defamatory material, copyright and harassment.
- Where you upload, post or publish content on the internet as part of your role at the BBC, you must comply with the BBC Editorial Guidelines.
- When you provide content (on the internet, intranet or in emails) you must ensure that it is clear when you are expressing a personal view and when you are expressing the view of the BBC. In particular where appropriate you must abide by the BBC Editorial Guidelines.

7 Accessing Offensive Material for Journalistic or Research Purposes

In order to access offensive material you must do the following:

- complete an AOMJR form;

- receive full authorisation for your request; and
- comply with the AOMJR guidelines http://home.gateway.bbc.co.uk/is/AOMJR Approval Guidelines.doc.

8 Email

8.1 Sending emails

- You must not send or solicit any material that is pornographic, obscene, hateful or defamatory.
- You must not send or solicit any material that is intended to harass or intimidate any other individual.
- As with any document, when composing and sending email, you must consider whether you are likely to cause offence, to enter into a contract (intentionally or otherwise), or to commit to any action. With email message often being drafted and sent more quickly than letters and faxes, these considerations become more vital. Email correspondence should be drafted with the same care and attention as all other normal correspondence.
- Avoid careless mistakes! Always check the email address of the recipient especially with sensitive or confidential emails.
- Remember that the recipient of an email may forward the message on to others.
- Do not forward emails which contain earlier emails without first ensuring that none of the earlier emails contain anything which would, justifiably, annoy a potential recipient, or does not contain confidential information.".
- Do not make adverse comments in an email about a colleague or any person with whom you are working.
- You should note that emails are admissible as evidence in legal proceedings and have been used successfully in court.
- Do not impersonate any other person when using email or amend messages received.
- You must not delete the BBC's automatic standard disclaimer on the end of each email.
- You are responsible for the content of all text, audio or images that you send via the BBC Equipment.
- You must not send anonymous emails from BBC Equipment.
- Do not create email congestion by sending chain emails, trivial or unnecessary personal messages or by copying emails to those who do not need to see them.

8.2 Managing your email account

- You should check your inbox regularly or ensure that someone else is able to check your inbox using delegated authority.
- Where appropriate, a manager may obtain access (under an Information Security Request) to an email account of a member of their team where that member is absent, to ensure that business correspondence is effectively dealt with.
- Set up delegations so that at least one other person has access to your email in case you are absent.
- Do not provide any delegate with the right to view messages marked as private. This will ensure that messages sent to you as private cannot be read by anybody other than yourself.
- Do not send an email on behalf of any other person other than by using delegation rights.

- You should be aware that the internet is not a secure network and so it is possible for others to read emails as they pass through it. Should you require any email to be encrypted before sending, please contact ISM@bbc.co.uk
- You must protect attached documents - contact ISM@bbc.co.uk for details on best practice in this area.
- Email messages are an increasing source of viruses, particularly viruses sitting within attached documents. If you think that you have been sent a document that contains a virus particularly if you have received an email from an unknown external source or the email appears suspicious, you should contact your local service desk immediately. You must not open any suspect email or attachments.
- You must delete emails on a daily basis from your inbox to prevent a build-up. A build up can prevent you from effectively monitoring and managing your emails.

9 External email accounts

- External email accounts are email accounts which are usually web-based e.g. Hotmail, Yahoo, Gmail. These accounts may not be secure as they bypass the BBC's external antivirus scanning systems. It should be noted that these external companies may retain a copy of the mail, over which the BBC has no control.
- You must not use external email accounts to transfer confidential information for home use.
- You must not use your 'Out of Office Assistant' to forward automatically messages to any external email system without the prior agreement of the Information Security Department ism@bbc.co.uk

10 Confidentiality

- Generally, confidential information includes any information which is not available to the public. It includes information which would damage the business of the BBC if it became known to those outside the BBC. It may also include the information of third parties who are providing services or working in partnership with the BBC. This also covers information where it is confidential internally, such as appraisals etc.
- It's important that you take all necessary measures to maintain the confidentiality of information that is transmitted or contained in BBC Equipment including through using encryption and ensuring the security of hardware (including laptops). Contact ism@bbc.co.uk for details on how to do this.
- You should limit the number of people to whom you send confidential information to only those with a genuine need to know.
- You should label confidential communications as "CONFIDENTIAL" and state explicitly how you expect the recipients to deal with this information.
- You must never post confidential or sensitive BBC information on any internet site, including social networking sites (e.g. Facebook).
- Before sending confidential information by email, consider sending it by internal post or courier instead.

11 Security

11.1 Only access information that you have a genuine need to know

- You must only access information on BBC Equipment and systems about which you have a genuine business need to know.
- If you access information to which you are not authorised you may be committing a criminal offence (e.g. under the Computer Misuse Act), as well as a breach of this Policy.

11.2 Hardware, Software and Programs

- Do not download ANY software or any unauthorised programs without following the process set out at http://sbsportal.bbc.co.uk/alarms/forms/softwareevaluation.html You should note that the use of unlicensed software can also have severe legal implications since you may be infringing someone else's copyright or importing a virus.
- Do not open e-mails or attachments from non-trusted sources
- Do not import any non-text file (including files received as email attachments) on to your system without first checking them for viruses using approved virus detection software.
- BBC Equipment must not be modified in its setup nor have additional software installed unless approved as set out at http://home.gateway.bbc.co.uk/is/DSFTI.htm.
- You may not copy, change, or transfer any software provided by the BBC without permission.

11.3 Accessing other people's accounts

- Under no circumstances should you access the accounts of another BBC User unless specifically authorised to do so through delegation rights or as provided by the process set out at http://home.gateway.bbc.co.uk/is/rtrd.htm

11.4 Passwords

You must keep all passwords to BBC Equipment safe. Don't write them down in any manner that would make it easy to decipher. Do not tell anyone your login details or password. You must create your passwords in accordance with http://guidelines.gateway.bbc.co.uk/dq/is/password_policy.shtml. If you believe that your account has been accessed without your knowledge, then you should change your password and contact the Head of Information Security immediately at ism@bbc.co.uk. If you need to store lots of passwords please use the software product 'password safe' which is available as freeware on the alarms website.

12 Defamation

- Defamation is the publication of a statement that adversely affects the reputation of a person or an organisation. Publication can be by way of the internet or by email.
- You must not send or circulate, internally or externally, any information that is defamatory. In particular, you must not send or circulate, internally or externally, any information that contains negative comments about an individual or organisation without first checking that the contents of the information are accurate.
- A person or organisation defamed can sue you or the BBC for damages. Although the law recognises that it is a defence if the information is 'true', the onus is on you or the BBC to show that.

13 Copyright

- The owner of copyright has the exclusive rights in certain works such as documents, articles, books, plays and musical compositions, so that they cannot be copied or used in certain ways without the consent of the copyright owner.
- You must not download, store, copy or transmit to third parties the works of others (including MP3 and other media files) without their permission as this may infringe copyright. Copyright is most likely to be breached when you download material from the internet or copy text and attach it to an email message.
- You should note that you infringe someone's copyright where you use either the whole or a substantial part of their work without permission subject to certain exceptions. Please consult the Editorial Guidelines or contact the controller Editorial Policy.

14 Harassment

- All BBC staff must be allowed to work in an environment free from harassment of any kind. This includes (but is not limited to) sexual and racial harassment and harassment on the ground of sexual orientation, age, religion, disability and marital status. Harassment affects morale and prevents a person fulfilling their full potential in their work.
- Sexual harassment is unwanted conduct of a sexual nature, or other conduct based on sex affecting the dignity of men and women at work. In the context of this policy this includes sending messages with sexually suggestive material, sexual propositions or abuse of a sexual nature.
- Racial harassment is unwanted conduct based on race, colour, ethnic or national origin affecting the dignity of men and women at work. In the context of this policy this includes sending messages containing offensive insults or 'jokes' based on race and abuse of a racial nature.
- You must not send messages which contain sexual or racist material or which are otherwise abusive or could constitute harassment on any other ground. It is important to note that the recipient may determine what is and is not offensive.
- Harassment is a criminal offence for which the harasser can be imprisoned. Victims of harassment may be able to claim damages from the harasser and the BBC.

15 Breach of this policy and applicable laws

The BBC reserves the right to implement appropriate disciplinary measures against you in response to any breach of this policy.

Further, as mentioned above, some breaches of this policy may also be illegal. For instance:

- If you knowingly or recklessly obtain or disclose personal information without the BBC's consent, you may be guilty of an offence under the Data Protection Act 1998;
- If you introduce viruses into the BBC Equipment, you may be guilty of an offence under the Computer Misuse Act 1998; and
- If you use someone else's copyright protected material without their consent, you may be guilty of an offence under the Copyright, Designs and Patents Act 1988.
- You must comply with the rules under all relevant legislation.

The BBC will comply with reasonable requests from law enforcement and regulatory authorities for the disclosure of information relating to an individual's use of the internet and other systems.

16 Telephones

The BBC provides telephones (including mobile phones and PDAs) for its business. You may use the BBC's telephones for a reasonable level of short personal calls. The following behaviour may result in disciplinary action:

- Long telephone conversations except in exceptional circumstances. If you think you may need to make an urgent long telephone call you should seek permission first;
- Continued excessive use of the BBC's telephones even for short personal calls;
- Overseas calls, other than for the BBC's business; and
- Calls to premium rate numbers.

Personal calls should be kept to a minimum since the BBC telephone lines should be kept clear for business calls.

17 Monitoring

17.1 Why does the BBC monitor communications?

The BBC is ultimately responsible for all business communications but will, as far as possible and appropriate, respect your privacy while you work. It is important, however, that you understand that the BBC may monitor your communications and use of BBC Equipment for reasons which include:

- Ensuring that the BBC's procedures and policies (including Editorial Policies) are adhered to;
- Monitoring standards of service and staff performance;
- Record keeping;
- Preventing or detecting unauthorised use of BBC Equipment and systems, including compliance with this policy;
- Complying with legal obligations and preventing and detecting criminal activities; and
- Maintaining the effective operation of the BBC's communications systems.

17.2 What does the BBC monitor?

The BBC may monitor telephone, email and internet traffic data (i.e. sender, receiver, subject, attachments to emails, numbers called and duration of calls and files downloaded from the internet) at a network level (covering personal and business communications). The BBC may also monitor the content of communications where it appears to the BBC that the use of the BBC Equipment is being abused or used inappropriately. A manager may monitor the emails received by a member of his or her team when that member is absent under an Information Security Application to ensure business correspondence is dealt with.

You should be aware that this monitoring may reveal personal information about you, for instance which websites you visit, the identity of people you email for personal reasons etc.

17.3 How does the BBC monitor?

BBC Investigations Service, BBC People and Siemens (as the BBC's service provider or 'data processor' processing data on the BBC's behalf) monitor communications in two ways:

- Pro-actively – when they investigate a person's online actions as part of an ongoing investigation. Before beginning to monitor, they will go through a number of processes to ensure that the steps taken are reasonable and proportionate.
- Monitoring of past communications – this is an examination/analysis of past communication that can be done as part of an ongoing investigation or randomly. e.g. the BBC may request Siemens to perform a check on bandwidth use. If one user has a high level of bandwidth use, the BBC may investigate further. In some circumstances this has shown that BBC Users have been downloading pornography in contravention of this policy (and the law, in some cases).

The BBC may use any information it receives via this monitoring process to investigate any claims of breach of this policy or any law and to instigate appropriate disciplinary or legal proceedings.

17.4 Who monitors and what is done with information elicited from monitoring?

It is the responsibility of BBC Investigation Service to carry out monitoring to prevent or detect unauthorised use of BBC Equipment and systems, compliance with legal obligations, and preventing and detecting criminal activities.

It is the responsibility of BBC People to carry out all other monitoring.

The BBC will only disclose information obtained through monitoring to:

- a relevant external agency if required by law; or
- to those directing the investigation i.e. BBC management or BBC People, for the purposes of criminal, civil or disciplinary purposes.

17.5 How long is monitoring data held?

Information obtained through monitoring will only be held for as long as it is necessary to complete enquiries. Where information is part of disciplinary proceedings, the information will be kept in accordance with the retention period for such proceedings.

17.6 Will I know if I am being monitored?

Wherever reasonable the BBC Investigation Service, BBC People or your manager (if appropriate) will consult with you about any suspected breach of this policy before any action is taken against you. However, it may not be practical to consult with you beforehand where illegal behaviour or gross misconduct is suspected.

18 Questions

If you have any questions about this policy please contact Head of Information Security on ism@bbc.co.uk .

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 _____

_____

_____

_____

_____

BBC

BBC

Appendix A. Document History

Version	Date	Author	Changes
0.5	18/06/2004	Alan MacGechan	Draft Version
1.0	20/06/2004	Julia Harris	Draft version for distribution to ISSG
1.1	16/07/04	Julia Harris	First version including comments from ISSG
2.0	22/07/04	Julia Harris	Second version following changes in BBC structure
3.0	20/11/07	Lucy McGrath	Amalgamation of AUG and General user rules, intending to ensure easy to read and consistent advice given.
3.1	26/11/07	Nancy Dickie	Changes from Legal
3.2	27/11/07	Lucy McGrath	Added links to Info Sec and DQ policies where relevant
3.3	3/12/07	Lucy McGrath	Added social networking references
3.4	25/1/2008	Kit Kitson	Investigations Changes
3.5	12/2/2008	Lucy McGrath	Monitoring changes (have taken out phone references after advice from BBC People)
3.6	15/2/2008	Lucy McGrath	Changes after discussion with Julia Harris (head of Info Security)
3.7	21/2/2008	FFW	External legal review
3.8	11/03/08	Julia Harris	Placing into FM&T format and final security edits
03.09	25/05/08	Julia Harris	Further updates following comments from DQ change control – CR Ref 08_006