# Acceptable Use of Information Systems Policy

## Overview
- This policy defines appropriate and inappropriate use of BBC Information Systems.
- BBC Information Systems are defined as BBC systems, devices, services (e.g. Internet, email, “bring your own device” (when connected to BBC systems) and telephony), applications, information in logical and physical form, as well as any other BBC equipment.
- This includes service providers’ systems or equipment when provided to the BBC.
- Inappropriate use of BBC Information Systems exposes the BBC to risks such as loss, disclosure or corruption of information; compromise of network systems and services as well as inappropriate or unauthorised access.
- These risks could result in reputational damage to the BBC, as well as fines or claims for damages resulting from a breach of legislative, regulatory or contractual obligations.

## Audience
- Anyone who has access to BBC Information Systems however they are employed or under a term of contract with the BBC, including via third parties.
- It also extends to information held on behalf of third parties and partners.

## Owner
- Head of Information Security, Head of Data Protection, Head of Legal & Business Affairs Future Media.

## Updated
- 27/04/2016
Contents

1 Introduction .................................................................................................................................. 3
2 General use of BBC information systems .................................................................................. 4
3 Protecting BBC Restrict information ....................................................................................... 5
4 Secure use of the Internet .......................................................................................................... 5
5 Secure use of electronic communications .................................................................................... 6
6 Physical security .......................................................................................................................... 6
7 Passwords ..................................................................................................................................... 7
8 Removable storage media ............................................................................................................. 7
9 Secure configuration of BBC Information Systems ..................................................................... 8
10 Communications services .......................................................................................................... 8
11 Monitoring of BBC Information Systems .................................................................................. 8
12 Investigation of individuals using BBC Information Systems ................................................ 9
13 Defamation ................................................................................................................................ 10
14 Harassment ............................................................................................................................... 10
15 Copyright .................................................................................................................................. 10
16 Exception management ............................................................................................................... 10
17 Reviewing and amending this policy ......................................................................................... 10
18 Definitions .................................................................................................................................. 11
19 References .................................................................................................................................. 11
20 Document control ....................................................................................................................... 13
1 Introduction

Information is an asset, and like any other business asset it has a value and must be protected. This value is not just financial but is based on the consequences of the information or Information Systems, being compromised and the negative impact that would have on individuals and the BBC. The BBC will continue to protect its interests against the inappropriate use of its Information Systems.

For the purpose of this policy, Information Systems is defined as BBC systems, devices, services (e.g. Internet, email, “bring your own device” (when connected to the BBC systems) and telephony), applications and information in logical and physical form as well as any other BBC equipment. This also includes service providers’ systems/equipment when provided to the BBC.

This Acceptable Use of Information Systems policy is part of the Information Security Policy Framework and should be read in conjunction with the BBC Editorial Guidelines, the BBC Data Protection Handbook and any other relevant policies as mentioned in this document.

It is not the intention of this policy to impose unnecessary restrictions on you that conflict with the BBC’s culture of openness, trust and integrity. However, your awareness and cooperation is essential for maintaining the effective security of BBC Information Systems.

1.1 Purpose

This policy has been written to help you understand what the BBC defines as appropriate and inappropriate use of its Information Systems and to remain within those limits during your work with the BBC. Inappropriate use exposes the BBC to risks such as malware attacks, inappropriate or unauthorised access, corruption, loss or disclosure of information, or a compromise of network systems and services. These risks could result in public embarrassment for the BBC as well as fines and/or claims for damages resulting from a breach of legislative or contractual obligations.

It is important that you understand what is required of you and what you need to do to comply with this policy. You must be aware of your responsibilities and understand that failure to comply with this policy may result in disciplinary action being taken against you including dismissal and/or legal action.

If you have any questions about this policy please contact your line manager first or BBC Information Security.

1.2 Audience

This policy applies at all times when using BBC Information Systems and not just during your normal working hours.

This policy applies to anyone who has access to BBC Information Systems however they are employed or under a term of contract with the BBC, including via third parties. In effect, this policy applies to anyone working in the BBC Group regardless of your location. It also extends to information held on behalf of third parties and partners.
1.3 Scope

This policy applies to all BBC Information Systems as well as to any other device used to store or process BBC information. This policy also applies when using your own device to store, access or process information on BBC Information Systems.

2 General use of BBC information systems

2.1 Your behaviour: You must act honestly and with integrity at all times to protect the BBC’s reputation, in accordance with the BBC values.

2.2 Your role: You must understand your role and responsibilities with regard to BBC Information Systems. If this is unclear then you must consult your line manager.

2.3 Information security incidents: You must report all actual or suspected information security incidents immediately to BBC Information Security using the Information Security Incident Reporting Procedure. Where the incident involves personal information then you must also immediately report the incident to the Data Protection team.

2.4 Business use: You must not use BBC Information Systems for any business activities which are not related to your work at the BBC.

2.5 Personal use: You are allowed reasonable and limited personal use when using BBC Information Systems however, they must not be used to take part in online gambling. The BBC may decide to limit your ability to use BBC Information Systems for personal use where there is possible, or actual, interference with BBC business. This would be decided by your line manager with input from BBC People. Any personal use of BBC Information Systems is at your own risk.

2.6 Information privacy: Your personal privacy is respected and access controls are in place, but you must understand that the BBC may monitor your use of BBC Information Systems for security purposes and also to check your compliance with this policy at any time and potentially without notifying you. Please see the Monitoring section for further details.

2.7 Accessing BBC Information Systems: When accessing BBC Information Systems you must only carry out the activities you are authorised to do. You must not access or try to access any BBC Information Systems where you are not authorised to do so, for example logging into accounts which are not yours. Doing so may be a crime under the Computer Misuse Act 1990.

You are responsible for any activity carried out under your username. You must not let anyone else use your BBC Information System when logged in with your own username and password unless all of the following apply:

- it is for IT support or delivering presentations/training where multiple people need to use one device;
- it is for a limited period of time; and
- it takes place under your direct and continuous supervision.

2.8 Offensive material: You must not knowingly attempt to visit, send or store any website, electronic communications or information on BBC Information Systems that is likely to cause harassment, alarm or distress. This includes sites and information
which may contain nudity, pornographic, obscene, indecent, hateful or other offensive material. Authorisation to access such material for business or journalistic purposes must be applied for using the Accessing Offensive Material for Journalistic or Research Purposes (AOMJR) process on Gateway.

3 Protecting BBC Restrict information

3.1 Working with BBC Restrict information: You must not print, share, post, publish, upload or email any information that is likely to be, or has already been classified as BBC Restrict information unless you are authorised to do so. If you need to handle BBC Restrict information then you must take the appropriate measures to maintain its confidentiality, e.g. by using encryption or ensuring its physical security. The BBC Information Classification & Handling Standard sets out how BBC information should be classified and handled.

4 Secure use of the Internet

4.1 Unauthorised software: The integrity and security of the BBC and its Information Systems could be impacted by downloading unauthorised, illegal or malicious software. You must not knowingly download, install or run any software on BBC Information Systems without first obtaining appropriate authorisation (for example by contacting your local IT Service Desk), unless the software is listed as approved on the Software Catalogue. If you need to install software you must contact the BBC Software Compliance Team. When this is not possible (for example outside normal working hours) they must inform their managers and Information Security by e-mail and ensure that the software is removed immediately after the specific task is completed.

4.2 Mobile applications: You must only download or install mobile applications onto BBC Information Systems from approved and reputable sources such as using the BBC Essentials service or an official application store or market. The integrity and security of the BBC and its Information Systems could be impacted by downloading unauthorised, illegal or malicious software. Further requirements on the use of mobile devices can be found in the Mobile Devices & Remote Working Policy.

You must read the information about an application in the application store before you download it and make sure that you are happy with the information it will be accessing. Any non-BBC application that wants to capture BBC information and store it must not be used. If you are in any doubt about whether to download an application, please contact BBC Information Security.

4.3 Social networking sites: You must use caution when using social networking for communication. You must use social networking sites in a professional and responsible manner and your contributions must comply with the Social Media and Social Networking statements within the BBC Editorial Guidelines.

It is your responsibility to ensure the social media account is protected by enabling the privacy settings available. Please see the BBC Social Media Security Standard for more detail.

4.4 Remote access: When you use a public/shared device to access BBC information remotely, you must reject any prompt to save your username or password in the browser for future use. You must also ensure that you log out of the remote access service completely when you are finished and close any open browser. Where possible you should log out of the device completely and either shut it down or restart
the device. It is your responsibility to ensure that your remote access occurs in an appropriate environment.

5 Secure use of electronic communications

5.1 Sending BBC Restrict Information: If you need to communicate any BBC Restrict information or information you consider sensitive then it must be encrypted. Further information and guidance can be found in the BBC Encryption Standard.

5.2 Use of personal communication accounts: You must not send or forward any restricted information to your personal communication systems (such as instant messaging, email, video communications), or use such an account for BBC business. If you have a requirement to work from home you should use BBC Webmail facilities or request the approved remote working solution from your local IT Service Desk.

5.3 Unnecessary e-mail traffic: You should not forward chain and spam communications as these cause unnecessary congestion on the network and also take up storage space.

You should also take great care before using “Reply All” to e-mail as this can generate very high levels of unnecessary traffic, or can lead to the distribution of sensitive information to recipients who do not have a legitimate reason to see it. Only use “Reply All” if every person copied into the email needs to receive it.

5.4 Suspect e-mail messages: The BBC is often targeted by suspicious emails which may introduce malicious software or trick you into giving up confidential information (phishing) e.g. your password, username or banking details. You must be careful when opening attachments or clicking on links in any communications you receive. This applies to emails from unknown sources, or unexpected communications from known sources. You must immediately report any suspect electronic communications to your local IT Service Desk.

5.5 E-mail Auto-forwarding: E-mail auto-forwarding to external addresses is not permitted from a BBC e-mail account unless an approved exception is authorised by BBC Information Security. Such an exception will only be granted for clear and compelling business reasons, and where all alternatives have been considered carefully and proved inappropriate.

6 Physical security

6.1 Access to premises: Access to BBC premises is for authorised personnel only through the allocation of either a BBC Identity Card or Visitors Pass. Please be aware of those in your office area and report any suspicious behaviour to BBC Workplace. Please wear your BBC Identity Card at all times while on BBC premises. Lost BBC Identity Passes must be reported to BBC Workplace immediately so that the pass may be temporarily deactivated. Access to BBC premises may be recorded for security purposes through CCTV and access management systems. Any attempted unauthorised access to areas which are restricted for either security or health and safety reasons is a violation of this policy.

6.2 Keeping your desk clear: You must make sure all restricted information is locked away when you leave the office in accordance with the BBC’s clear desk policy.
6.3 **Protecting your equipment:** You are responsible for ensuring the security and safe keeping of BBC Information Systems and other devices containing BBC information; particularly at non-BBC locations such as your vehicle, at home, when on the train, having a coffee etc.

6.4 **Safe storage:** If you need to leave any portable BBC Information System (such as phones, mobiles, laptops and tablets), or any other device containing BBC information, in the office overnight or when you have finished working for the day, then you must lock it into storage. If you are at a non-BBC location then you must take similar measures.

6.5 **Shoulder surfing:** In public places, such as trains or coffee shops, you must be aware of others who may be able to view your password entry, screen or papers. You must take appropriate precautions particularly with using Restricted information in such circumstances.

6.6 **Protecting your screen:** If you need to leave BBC Information Systems, or other devices containing BBC information, unattended then you must activate a password protected screen lock.

6.7 **Shutting-down your computer:** You must always shut-down your computer, and wait until it has fully shut-down, when you have to leave it unattended for long periods of time or when not using it outside of your normal working hours.

6.8 **Reporting theft or loss:** You must immediately report all lost or stolen BBC Information Systems, or other devices containing BBC information, to your local IT Service Desk and BBC Investigation Service by following the link in the references section. Where the theft or loss of a physical item involves personal information then you must also immediately report the incident to contact the Data Protection team as per the link in the references section.

7 **Passwords**

7.1 **Creation of strong passwords:** You must create your unique passwords in accordance with the BBC Password Policy.

7.2 **Keep passwords secure:** You must keep all your passwords safe. Don’t write them down in any manner that would make it easy to decipher and don’t tell anyone your login details or password – including your manager or IT. This includes all information systems and websites i.e. social media. Any activity carried out on your password protected account will be deemed to be your activity unless there is evidence to the contrary.

7.3 **Exemptions and delegated authority:** We recognise there may be instances when you do need to share your password, however you must only do this with a valid business justification and only after notifying BBC Information Security by emailing Information.Security@bbc.co.uk. You must thereafter change your password at the earliest opportunity.

8 **Removable storage media**

8.1 **Using removable storage:** If you are copying BBC Restrict information to removable storage media (e.g. USB drives, CD/ DVDs etc.) then you must encrypt it in compliance with the Data Encryption Standard and keep it secure at all times.
8.2 **Removable media from third parties:** You must advise any third party wishing to send you any restricted information on removable media to use encryption as outlined in the BBC Encryption Standard. If you have received the removable media unencrypted then you must copy the information to your BBC Information System and immediately encrypt the removable media using the BBC's USB encryption tool.

9 **Secure configuration of BBC Information Systems**

9.1 **Security tools on BBC Information System:** You must not attempt to bypass or tamper with any of the security measures that the BBC has in place.

9.2 **Configuration of BBC Information Systems:** You must not modify the configuration of BBC Information Systems nor install additional software unless you have been authorised to do so.

9.3 **Authorised information systems:** Only equipment and media (including removable storage media) that has been authorised by the BBC must be used to directly connect to BBC Information Systems, including the network.

10 **Communications services**

10.1 **Personal use:** You are permitted to use the BBC's communications services, including but not limited to telephones, mobile phones and Skype, for a reasonable amount of personal use, however this must be kept to a minimum since the communication services must be kept available for business use. Any abuse of the communications service, such as excessive, long, premium or long-distance usage may result in disciplinary action. If you have an exceptional circumstance then you must seek authorisation from your line manager.

11 **Monitoring of BBC Information Systems**

11.1 **General monitoring:** Both specialist IT staff and automated computerised systems are used to monitor BBC Information Systems including but not limited to BBC telephones, mobile devices, computers, CCTV, communications systems and Internet systems. Systems have been implemented to automate monitoring where viable to ensure real-time protection and minimal human intervention. Digital information and data passing through these systems are subject to on-going and random monitoring for system security and integrity reasons in order to:

- maintain the effective operation of the BBC’s communications systems;
- check on standards of service and quality of staff performance; and
- ensure compliance with this policy.

11.2 **Specific monitoring:** Your communications may be monitored when it appears that BBC Information Systems are being misused or used inappropriately. There may be other reasons why your communications are monitored, e.g. in your absence after a formal request is made for access to emails and/or data files in your mailbox or on your device to ensure business correspondence is dealt with. This will be in accordance with an authorised investigation (see section 12).

11.3 **Monitoring personnel:** Access to information obtained through monitoring is controlled and limited to trained and designated staff to ensure an acceptable level of confidentiality and privacy.

11.5 The BBC Investigation Service manages access to data through a formal application process and has authority to permit or reject the monitoring request.

11.6 In every case, the requester will make a written application to ensure the criteria for monitoring will satisfy the requirements of relevant legislation, to ensure monitoring is necessary, reasonable and is a proportionate response in all the circumstances.

11.7 The BBC Investigation Service will complete a formal record of the authority or refusal, setting out the data requested and the criteria upon which the decision was made. This process is subject of formal validation, being overseen and administered by the Head of the BBC Investigation Service. Ultimately, this process is subject to independent audit.

11.8 You can find out more about using data as part of a fact finding investigation in the Guide to Disclosure of Personal Information.

12 **Investigation of individuals using BBC Information Systems**

12.1 **Why we may investigate your use of BBC Information Systems:** The BBC respects your privacy and does not investigate your activity on BBC Information Systems without proper grounds. The BBC however is ultimately responsible for all communications and devices on BBC Information Systems. It is therefore important that you understand that the BBC can investigate your BBC communications and your use of its Information Systems for reasons which include:

- any serious incident where the investigation of the BBC, or its staff, is necessary in the public interest;
- to comply with legal obligations and the prevention or detection of criminal activities;
- to ensure that the BBC’s policies and procedures are adhered to;
- to prevent or detect unauthorised use of BBC Information Systems; and
- when necessary, to conduct authorised investigations into an individual user.

12.2 **Investigation of past communications:** Your past communications may be examined or analysed as part of on-going operational needs or investigations. The BBC may use any information it obtains via this process to investigate any claims of breach of this policy or any law and to instigate appropriate disciplinary or legal proceedings.

12.3 **Notification of investigations:** Wherever reasonable, and if appropriate, we will consult 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.

12.4 **Personal information during investigations:** You should be aware that investigations may reveal personal information about you, for instance which websites
you visit, the identity of people you email for personal reasons etc. This will be held in confidence unless it is needed to form part of an authorised investigation.

13 Defamation

13.1 What is defamation: Defamation is the publication of a statement that adversely affects the reputation of a person or an organisation. The publication can be made using the Internet or any other electronic communication.

13.2 Defamation is not allowed: You must not send or circulate, internally or externally, any information that is defamatory. This includes 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. There is also a defence of fair comment – this is a complex area dealt with in BBC Editorial Guidelines, Section 18.4.1.

14 Harassment

14.1 Harassment is prohibited: The BBC will not tolerate any form of harassment and is committed to providing a workplace in which the dignity of individuals is respected. You must not knowingly attempt to send electronic communications or information on BBC Information Systems which may be deemed by the recipient to violate dignity or be perceived as intimidating, hostile, degrading, humiliating or offensive, as set out in the BBC Bullying & Harassment Grievance Policy. Any harassment will be dealt with under the BBC’s Disciplinary Policy and may result in disciplinary action being taken and could potentially be a criminal offence.

15 Copyright

15.1 Protecting copyright: You must not download, store, copy or transmit the works of others without their permission as this may infringe copyright. Please consult the BBC Editorial Guidelines for further information. 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.

16 Exception management

16.1 Exceptions process: Where it is not possible to apply or enforce any part of this policy then a BBC Dispensation Request must be completed and returned to BBC Information Security. BBC Information Security will review the business justification and advise on the risks involved. Policy exceptions will only be issued when the Data Owner has signed off on the identified risks.

17 Reviewing and amending this policy

17.1 Amendments: The BBC reserves the right to review and amend this policy on a regular basis. This is the responsibility of Information Security Governance & Compliance.
18 Definitions

<table>
<thead>
<tr>
<th>BBC Information Systems</th>
<th>Systems, devices, services (e.g. Internet, email, and telephony), applications and information in logical or physical form as well as any other BBC equipment.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information Security Incident</td>
<td>An event that is likely to compromise the BBC by putting the confidentiality, integrity or availability of its information at risk,</td>
</tr>
<tr>
<td>Investigation</td>
<td>The BBC may investigate your communications and use of BBC Information System for reasons outlined in this policy.</td>
</tr>
<tr>
<td>Monitoring</td>
<td>Automatic system monitoring of telephone, email, Internet and network traffic data and also monitoring of individual communications, which may be done on an exceptions basis on particular occasions.</td>
</tr>
<tr>
<td>Removable media storage</td>
<td>Any form of media able to record data electronically and capable of being connected to BBC systems, including but not limited to USB disk, CD/DVD, Memory Card, Smartphone disk</td>
</tr>
<tr>
<td>Restricted Information</td>
<td>Personal data, Bank accounts, Employee health records, Contracts, Data covered by NDAs, Commercially-sensitive data. The BBC Information Classification &amp; Handling Standard contains more detail.</td>
</tr>
</tbody>
</table>

19 References

Contact Information Security (information.security@bbc.co.uk) for any additional documentation that has been referenced within this policy.
### 20 Document control

<table>
<thead>
<tr>
<th>Date</th>
<th>Version</th>
<th>Author</th>
<th>Changes/Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>11/04/2013</td>
<td>1.0</td>
<td>AR</td>
<td>Final version (approved by ISCB)</td>
</tr>
<tr>
<td>18/10/2013</td>
<td>1.1</td>
<td>AC</td>
<td>Minor Updates following feedback from NJC</td>
</tr>
<tr>
<td>13/11/2013</td>
<td>1.2</td>
<td>AC</td>
<td>Incorporated wording supplied by Investigations Team for monitoring section and added policy statement for external email auto-forwarding agreed by ISCB on 14/10/2013</td>
</tr>
<tr>
<td>20/11/13</td>
<td>2.0</td>
<td>AC</td>
<td>Revised version agreed for publication</td>
</tr>
<tr>
<td>02/09/2014</td>
<td>2.1</td>
<td>VG</td>
<td>Minor rewording and updated formatting for Gateway policy project. Updated section 2.5 to reference online gambling. Updated section 2.7 to add second paragraph and agreed exceptions to this policy statement. Updated section 4.3 to reference the new Social Media security Standard. Updated section 5.3 to remove reference to BCC’d and to emphasise appropriate use of ‘Reply All’. Split section 5.3 into 2 and created 5.4 as original section 5.3 covered 2 separate issues.</td>
</tr>
<tr>
<td>24/09/2014</td>
<td>2.2</td>
<td>VG</td>
<td>Updated ISGC to BBC Information Security to reflect the change in the team name</td>
</tr>
<tr>
<td>28/10/2014</td>
<td>2.3</td>
<td>VG</td>
<td>Updated 6.4. Approved at the ISCB meeting on 27/10/2014.</td>
</tr>
<tr>
<td>18/11/2014</td>
<td>2.4</td>
<td>VG</td>
<td>Updated 4.2 following the ISCB meeting on 18/11/2014. Updated 16.1 to reference the Dispensation Process.</td>
</tr>
<tr>
<td>10/02/2015</td>
<td>2.5</td>
<td>VG</td>
<td>Updated 2.5 following an issue raised by BBC Employment Legal. Updated 4.2 following the ISCB meeting on 28th January 2015.</td>
</tr>
<tr>
<td>27/04/2016</td>
<td>2.6</td>
<td>AU/VG</td>
<td>Updated links following changes to Gateway. Added reference to BBC Restrict in line with the new...</td>
</tr>
<tr>
<td></td>
<td></td>
<td>BBC Information Classification &amp; Handling Standard.</td>
<td></td>
</tr>
</tbody>
</table>