Effective from: 24/06/2024

Policy owner: Chief Information Security Officer

Owner's department: Information Security

Contact details for queries: Information Security Policy

Version control: 4.2

‘One minute’ policy summary

Purpose & Scope:
The purpose of this policy is to prevent the compromise of BBC information systems through misuse.

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 Code of Conduct the BBC Data Protection Handbook, the BBC Technology and Software policies as well as any other relevant policies as mentioned in this document. Those employed within BBC Studios and its subsidiaries must also follow BBC Studios specific equivalent policies.

Target Audience:
This policy applies to all BBC employees, BBC Studios and anyone that has access to BBC Information Systems, however they are employed or engaged 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.

Impact on risk:
This policy has been written to help understanding of what the BBC defines as appropriate and inappropriate use of its Information systems. 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 reputational damage for the BBC as well as fines and/or claims for damages resulting from a breach of legislative or contractual obligations.

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

Key points of this policy:

1. Phishing - You must be vigilant when opening attachments or clicking on links in any communications you receive. The BBC is often targeted by scam emails (phishing) which may introduce malicious software or trick you into giving up confidential information e.g. your personal credentials.

2. Personal Communication - You are allowed reasonable and limited personal use when using BBC Information Systems; however, you must always abide by all relevant software licensing agreements. BBC Information Systems must also never be used to take part in online gambling or any other online activities which could be perceived as

offensive, indecent, hateful or unlawful. All personal use is done at your own risk. 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.

You must not use a personal email account for your BBC work. Secure options for accessing your BBC email on the go or at home are available.

You must not use your BBC email address to sign up for or link to any external service that will be used exclusively for personal reasons. External services include (but are not limited to) banking, shopping, social media, cloud services etc. See Sections 4, 7 and 12 for further details on personal use of BBC Information Systems.

3. 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

Information Security Inbox	information.security@bbc.co.uk	-

Approval
Approved by: The InfoSec Policy Review Panel on: 24/06/2024

Contents

BBC Acceptable Use of Information Systems Policy

1. Policy purpose and scope

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

	This includes information that must be publicly disclosed under the Freedom of Information Act (FOIA).
PROTECTED Information	BBC Protected information is defined as any information that does not fall under the definitions of BBC Restricted or BBC Public.
RESTRICTED Information	BBC Restricted information is defined as information which can only be handled through consultation with BBC Information Security such as: Journalistic sources who need to remain anonymous, information that could result in a threat to life, information that could prejudice national security or i

4.1 Your Behaviour: You must always act honestly and with integrity to protect the BBC's reputation, in accordance with the BBC Values, the BBC Code of Conduct

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 Device Security Policy.

7.2.1 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.

7.3 Social Networking Sites: You must use caution when using social networking for personal 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 whether or not your social media accounts are personal or identify you as connected with the BBC.

7.3.1 BBC Social Media accounts must have a designated account owner responsible for ensuring all relevant privacy settings are enabled. Please see the BBC Social Media Security Policy for more detail.

7.4 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.

7.5 Torrenting: Any use of torrenting software on BBC infrastructure (including through BBC approved remote access services) as part of your work activities must be approved by BBC Information Security. Copyright must also always be protected as detailed in Section 17.

7.6 Anonymity networks designed to conceal user identity and otherwise obfuscate security monitoring (e.g. TOR) must not be used to access BBC systems or information unless specifically approved by BBC Information Security.

8. Secure Use of Electronic Communications

8.1 All BBC information must be encrypted at rest and while in transit by only using approved BBC Systems.

When sending commercially sensitive, legally privileged, or personal data of any kind outside of the BBC additional encryption may be required.

Additional encryption may be required when sending special categories of personal information within the BBC.

Further information and guidance can be found in the BBC Classification Policy, Information Handling Standard and the Encryption Standard.

8.2 Use of Personal Communication Accounts: You must not send or forward any PROTECTED or 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 a BBC approved remote working solution from your local IT Service Desk.

8.3 Use of BBC Email Address You must not use your BBC email address to sign up for or link to any external service that will be used for personal reasons. External services include (but are not limited to) banking, shopping, social media, cloud services etc.

8.4 Unnecessary Email Traffic: You should not forward chain and spam communications as this causes unnecessary congestion on the network and 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. This can also 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.

8.5 Suspect Email 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 information.security@bbc.co.uk

8.6 E-mail Auto-Forwarding: E-mail auto-forwarding to external addresses is not permitted from a BBC e-mail account.

9.

10. Passwords

10.1 Creation of Strong Passwords: You must create your unique passwords in accordance with the BBC Password Standard.

10.2 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.

10.3 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 seeking approval from BBC Information Security by emailing information.security@bbc.co.uk. You must thereafter change your password at the earliest opportunity.

11. Removable Storage Media

11.1 Using removable storage: Use of external storage devices (e.g. USB drives, CD/ DVDs etc.) is not recommended. If unavoidable, removable storage being used to store PROTECTED information must be encrypted as soon as possible in line with the BBC Encryption Standard. You must contact BBC Information security for advice on handling RESTRICTED information.

11.2 Removable Media from Third Parties: You must advise any third party wishing to send you any personal or RESTRICTED information on removable media to use encryption as outlined in the BBC Encryption Standard. If you have received an unencrypted removable media device then you must copy the information to your BBC Information System and immediately encrypt the removable media by following the instructions here.

12. Secure Configurations of BBC Information Systems

12.1 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.

12.2 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.

12.3 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.

13. Communications Services

13.1 Personal Use: You are permitted to use the BBC's communications services, including but not limited to telephones, mobile devices and internet browsers for reasonable and limited personal use. This use must be kept to a minimum. 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.

13.2 BBC communications services must never be used for gambling.

14. Monitoring of BBC Information Systems

14.1 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:

!

to prevent or detect unauthorised use of BBC Information Systems; and

when necessary, to conduct authorised investigations into an individual user.

15.2 Investigation of Past Communications: Your past communications may be examined or analysed as part of on-going operational needs, investigations or as part of a data subject access request. 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.

15.3 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.

15.4 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.

15.5 Notification of External Investigations: If your laptop, mov8e will be heation.

17. Harassment

17.1 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 Anti- Bullying & Harassment Policy. Any harassment will be dealt with under the BBC's Disciplinary Policy, BBC Code of Conduct and may result in disciplinary action being taken and could potentially be a criminal offence which may be reported by the BBC to the police or other appropriate law enforcement agency. Misconduct can be reported using the processes described in the BBC Whistleblowing Policy.

18. Copyright

18.1 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.

19. Internal/external links

Accessing Offensive Material for Journalistic or Research Purposes	https://onebbc.sharepoint.com/sites/fmt-InformationSecurity/Lists/AOMJR/NewForm.aspx?Source=https%3A%2F%2Fonebbc%2Esharepoint%2Ecom%2Fsites%2Ffmt%2DInformationSecurity%2FLists%2FAOMJR%2FAllItems%2Easpx&ContentTypeId=0x010058FA70617E925B40AFD8CBB278BD9B88&RootFolder=%2Fsites%2Ffmt%2DInformationSecurity%2FLists%2FA
Security and Investigations	https://staff.bbc.com/gateway/investigations/
Anti-Bullying and Harassment Policy	https://staff.bbc.com/gateway/policy/anti-bullying-and-harassment-policy/
BBC Encryption Standard	https://staff.bbc.com/gateway/infosec/policies/

BBC Information
Classification

18/11/2014 2.4