BBC Corporate Policy

BBC Acceptable Use of Information Systems Policy

Effective from: 08/09/2021

Policy owner: Chief Information Security Officer

Owner's department: Information Security

Contact details for queries: Information Security Policy

Version control: 4.1

‘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.

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 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. 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 harassment, alarm or distress. This includes sites and information which may contain nudity, pornographic, obscene, indecent, hateful or other offensive material. See Section 4.8: Offensive Material for further details.

4. **You must** Be vigilant and look after BBC equipment and information when you're in the office or out and about. **You must** report all lost BBC Information Systems, or other devices containing BBC information, to your local IT Service Desk. **You must** report all stolen BBC Information Systems to the BBC Investigation Service. Where the theft or loss of a physical item involves **personal information** then you must also immediately report the incident to the relevant team:
BBC Public Service – Data Protection Team
BBC Studios – Privacy Team

5. **You must** understand that the BBC may monitor your use of BBC Information Systems for security purposes and to check your compliance with this policy at any time and potentially without notifying you. See section 13: Monitoring of BBC Information Systems for further details.

Who can I contact for assistance?

Contact Information		
Name & Title	**E-mail**	**Contact Number**
James O'Connor – Information Security Specialist	James.oconnor@bbc.co.uk	-
Christopher Gamble – Information Security Officer	Christopher.gamble@bbc.co.uk	-
Information Security Inbox	information.security@bbc.co.uk	-

Approval
Approved by: The InfoSec Policy Review Panel on: 09/09/2021

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 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.

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. Terms and definitions

Term	Definition
BBC Information Systems	**Systems, devices, services (e.g. Internet, email, and telephony), applications and information in logical or physical form as well as any other BBC equipment.**
Information Security Incident	An event that is likely to compromise the BBC by putting the confidentiality, integrity or availability of its information at risk.
Investigation	The BBC may investigate your communications and use of BBC Information System for reasons outlined in this policy.
Monitoring	Automatic system monitoring of telephone, email, Internet and network traffic data. Also, monitoring of individual communications, which may be done in exceptional circumstances.
Removable Media Storage	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.
PUBLIC Information	BBC Public information is information that is already publicly available or information that has no negative impact on the BBC if it is disclosed. 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 information that could result in the BBC being taken off air if it was improperly accessed or disclosed.
Reasonable and Limited Personal Use	Doesn't affect your ability to carry out your role. The BBC incurs no additional costs. No security implications / breach of any BBC policy or terms of contract or licensing agreements.

3. Roles and responsibilities

It is the responsibility of everyone working for the BBC whether directly (e.g. Staff, FTC, Freelance or indirectly via Third Parties) to ensure the integrity of BBC Information Systems.

Further information about the BBC's wider approach to information security and roles and responsibilities can be found in the Corporate Information Security Policy.

4. General use of BBC information systems

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.

4.1 **Your Behaviour:** You must always act honestly and with integrity to protect the BBC's reputation, in accordance with the BBC Values as well as the terms and conditions of your employment.

4.2 **Your Role:** You must understand your role and responsibilities regarding BBC Information Systems. If this is unclear, then you must consult your line manager.

4.3 **Information Security Incidents:** You must report all actual or suspected information security incidents immediately to BBC Information Security.

4.3.1 Where security incidents involve personal information then you must also immediately report the incident to the relevant team:
BBC Public Service – Data Protection Team
BBC Studios – Data Privacy Team

4.3.2 In the case of an emergency security must be called on 0207 765 1666 (666 internally). If you are based at an international BBC site, local security guidelines must be followed. Refer to the Corporate Security page for more information on emergencies.

4.4 **Business Use:** You must not use BBC Information Systems for any business activities which are not related to your contracted work for the BBC.

4.5 **Personal Use:** You are allowed reasonable and limited personal use when using BBC Information Systems as long as you are in compliance with any applicable software licensing agreements.

4.5.1 Personal Use of BBC Approved Cloud Providers: Reasonable and limited personal use does not include personal use of approved BBC cloud providers. Non-work-related information must never be uploaded to these services.

4.5.1.1 BBC Information must never be uploaded to any cloud service which has not been approved by BBC InfoSec.

4.5.2 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.

4.5.3 BBC Information Systems must never be used to take part in online gambling.

4.6 **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 to check your compliance with this policy at any time and potentially without notifying you. Please see section 13 for further details.

4.7 **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 attempt 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.

4.7.1 You are responsible for any activity carried out under your BBC Login You must not let anyone else use your BBC Information System when logged in with your own username and password unless all 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; and
- it takes place under your direct and continuous supervision.

4.8 **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 otherwise offensive material. If access to this type of content is required for work purposes, the Accessing Offensive Material for Journalistic or Research Purposes (AOMJR) process must be followed.

4.9 **Actions Upon Termination of Contract:** BBC equipment and data, for example, but not limited to, laptops and mobile devices including telephones, smartphones, USB memory devices and CDs/DVDs, must be returned to the BBC at termination of contract. All BBC data or intellectual property created, developed or used by the employee during the period of his/her employment remains the property of the BBC and must not be retained beyond termination or reused for any other purpose unless otherwise agreed by the BBC. Team and line managers are responsible for ensuring this is carried out alongside removing IT access to BBC Information Systems. Please refer to the Checklist for an employee leaving the BBC for further information or contact BBC Information Security.

5. PROTECTED and RESTRICTED Information

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

6. Secure Use of the Internet

6.1 **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 BBC Software Compliance. 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.

6.2 **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 Device Security Policy.

6.2.1 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.

6.3 **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.

6.3.1 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.

6.4 **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.

6.5 **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.

6.6 **Anonymity networks** designed to conceal user identity and otherwise obfuscate security monitoring must not be used to access BBC systems or information unless specifically approved by BBC Information Security.

7. Secure Use of Electronic Communications

7.1 If you need to communicate any personal, commercially sensitive or legally privileged information outside of the BBC then encryption is required.

Encryption is also required when PROTECTED - Personal information is being sent internally.

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

7.2 **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.

7.3 **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 exclusively for personal reasons. External services include (but are not limited to) banking, shopping, social media, cloud services etc.

7.4 **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.

7.5 **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

7.6 **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.

8. Physical Security

8.1 **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 always wear your BBC Identity Card 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.

8.2 **Keeping Your Desk Clear:** You must make sure all **PROTECTED** and **RESTRICTED** information is locked away when you leave the office in accordance with the BBC's clear desk policy.

8.3 **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.

8.4 **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.

8.5 **Shoulder Surfing:** 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 **PROTECTED** or **RESTRICTED** information in such circumstances.

8.6 **Protecting Your Screen:** If you need to leave BBC Information Systems, or other devices containing BBC information, unattended within a BBC building then you must activate a password protected screen lock.

8.7 **Shutting Down Your Computer:** You must always shut down or lock your work computer before leaving it unattended for extended periods.

8.8 **Reporting Theft or Loss:** You must immediately report all lost BBC Information Systems, or other devices containing BBC information, to your local IT Service Desk. Stolen devices must be reported to the BBC Investigation Service. Where the theft or loss of a physical item involves personal information then you must also immediately report the incident to the relevant team:
BBC Public Service – Data Protection Team
BBC Studios – Data Privacy Team

9. Passwords

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

9.2 **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.

9.3 **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.

10. Removable Storage Media

10.1 **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.

10.2 **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.

11. Secure Configurations of BBC Information Systems

11.1 **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.

11.2 **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.

11.3 **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.

12. Communications Services

12.1 **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.

12.2 **BBC communications services** must never be used for gambling.

13. Monitoring of BBC Information Systems

13.1 **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.

13.2 Specific Monitoring: In accordance with an authorised investigation, your communications may be monitored when it appears that BBC Information Systems are being misused or used inappropriately (see Section 14). Your communications may be monitored for other reasons. This will be in line with our existing policies and relevant legislation.

13.3 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.

13.4 Authority to Monitor: The BBC adopts the guidance outlined in the Information Commissioners' Employment Practices Code and the Lawful Business Practice Regulation Part 3 – Monitoring at Work. The latter describes how organisations can seek to ensure adoption of the principles of the Regulation of Investigatory Powers Act 2000 and the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000.

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

13.4.2 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.

13.4.3 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.

14. Investigation of Individuals Using BBC Information Systems

14.1 Investigating 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.

14.2 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.

14.3 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.

14.4 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. Defamation

15.1 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.

15.2 **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.

16. Harassment

16.1 **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 and may result in disciplinary action being taken and could potentially be a criminal offence.

17. Copyright

17.1 **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.

18. 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 Policy	https://staff.bbc.com/gateway/policy/information-classification-policy/
BBC Information Handling Standard	https://staff.bbc.com/gateway/infosec/policies/
Data Protection Handbook	https://staff.bbc.com/gateway/policy/data-protection-handbook/
Studios DP Intranet Site	https://intranet.bbcstudios.com/privacy/introduction
Disciplinary Policy	https://staff.bbc.com/gateway/policy/disciplinary-policy/
Editorial Guidelines	http://www.bbc.co.uk/guidelines/editorialguidelines/
Information Security Incident Reporting	https://webapps.bbc.co.uk/gdpr/
Mobile Device Security Policy	https://staff.bbc.com/gateway/policy/mobile-devices-and-remote-working-security-policy/

Remote Working Standard	https://staff.bbc.com/gateway/infosec/policies/
Password Standard	https://staff.bbc.com/gateway/infosec/policies/
Personal Information Security Breach Reporting	https://staff.bbc.com/gateway/legal/data-protection/data-protection-breaches/
Studios Personal Information Security Breach	https://intranet.bbcstudios.com/privacy/report-a-data-breach
Studios DP & Cybersecurity Training	https://performancemanager.successfactors.eu/sf/learning?destUrl=https%3a%2f%2fbbcprod%2eplateau%2ecom%2flearning%2fuser%2fdeeplink%5fredirect%2ejsp%3flinkId%3dONLINE%5fCONTENT%5fSTRUCTURE%26componentID%3dCOU%2d10279%26componentTypeID%3dONLINE%26revisionDate%3d1619097300000%26fromSF%3dY&company=S001190811T2
Reporting Theft	https://staff.bbc.com/gateway/security/contact-us/
Reporting Loss	https://som-myit.onbmc.com/dwp/app/#/knowledge/KBA00009205/rkm
Request to Read Data	https://staff.bbc.com/gateway/investigations/contact-us/
BBC Social Media Security Standard	https://staff.bbc.com/gateway/infosec/policies/
How to Encrypt (Windows)	https://staff.bbc.com/gateway/infosec/documents/how-to-password-protect-encrypt-pc.pdf
How to Encrypt (Mac)	https://staff.bbc.com/gateway/infosec/documents/how-to-password-protect-encrypt-mac.pdf

19. Training requirements

Mandatory online Data Protection and Cyber Security training must be renewed every two years. BBC Studios DP & Cybersecurity Training can be found here.

20. Exceptions to Policy

Where it is not possible to apply or enforce any part of this policy then a BBC Residual Risk Acceptance must be completed and returned to the BBC Information Security team. The BBC Information Security team will review the business justification, fully assess the risk and advise on any action to be taken before formally issuing any recommendations to the Information Risk Owner (IRO).

Once the BBC Information Security team receives confirmation that the risk has been signed off by the IRO, a BBC Information Security RRA ID will be assigned. Any proposed changes or extensions to the original RRA request must be reported to the BBC Information Security team so that the request can be reassessed.

Without a BBC Information Security RRA ID being issued, an RRA is not considered as approved.

21. Policy assurance

The Information Security Policy Review Panel is responsible for the governance of infosec policy and forms part of the infosec policy approval process. Full details can be found on Gateway here.

22. Document Control

Document Name	Insert the name of the Policy		
Version	Enter the version number of the document; see Archive History below		
Source	Insert the owning Division/department		
Policy owner	Please insert the name and/or title of the person that is responsible for this policy There should be only one Policy Owner		
Approved by/Date	Date approved by Policy Owner		
Archive History:			
Date	**Version**	**Author**	**Changes/Comments**
11/04/2013	1.0	Atif Rafiq	Final version (approved by ISCB)
18/10/2013	1.1	Annamaria Cooper	Minor Updates following feedback from NJC
13/11/2013	1.2	Annamaria Cooper	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
20/11/2013	2.0	Annamaria Cooper	Revised version agreed for publication

02/09/2014	2.1	Vickie Greene	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.
24/09/2014	2.2	Vickie Greene	Updated ISGC to BBC Information Security to reflect the change in the team name
28/10/2014	2.3	Vickie Greene	Updated 6.4. Approved by ISCB on 27/10/14
18/11/2014	2.4	Vickie Greene	Updated 4.2 following the ISCB meeting on 18/11/2014. Updated 16.1 to reference the Dispensation Process
10/02/2015	2.5	Vickie Greene	Updated 2.5 following an issue raised by BBC Employment Legal. Updated 4.2 following the ISCB meeting on 28th January 2015.
27/04/2016	2.6	Ambi Ubhie/Vickie Greene	Updated links following changes to Gateway. Added reference to BBC Restrict in line with the new BBC Information Classification & Handling Standard.
24/01/2017	3.0	Dale Upton	DRAFT: Adapted to new template and added summary section '5 points keys about this policy'. Added section 2.9 Actions Upon Termination of Contract. Amendment to section 5.2 Use of personal communication accounts to not reference a specific solution, rather to use a BBC approved solution and where to seek guidance. Added section 5.3 Use of BBC email address. Amendment to section 6.5 Shoulder surfing to align with Information Classification and Handling Standard. Amendment to section 7.3 Exemptions and delegated authority to clarify the process for seeking approval when sharing passwords under a valid business reason.

08/08/2017	3.1	Dale Upton	Expanded Sections 1. Introduction and 2.9: Actions upon termination of contract. Expanded on the definition of 'Reasonable and Limited Personal Use'. Changed classification terminology and definition based on updated BBC Information Classification and Handling Standard. Added emergency contacts to section: 2.9 Reporting Information Security Incidents.
27/02/2018	3.2	Vickie Greene	Updated Section 16. with revised exceptions process standard wording.
07/12/2020	4.0	James O'Connor	Updated whole policy to new corporate format. Added requirements to abide by software licensing agreements.
23/08/2021	4.1	James O'Connor	Full review with HR, Legal and DP. Altered section 10.1 (Personal Use) Changed so as not to mention specific services, added that this must be done in compliance with any relevant BBC software licensing agreements. Added torrenting section 6.5. Added anonymised networks section 6.6 Updated in line with new versions of classification documents. Clarified/changed wording to in various sections to make things clearer.