Use of Technology Corporate Policy

Why this Policy matters

To fulfil our mission as a public service broadcaster, we must meet our legal and contractual obligations. This includes responsible and legitimate use of technology including: hardware, telephony and software.

There are financial, legal and reputational risks to the BBC when technology assets are purchased via unauthorised routes. The misuse and mismanagement of technology could lead to legal challenges, data breaches, security risks, significant costs or reputational damage.

By following this Policy, you contribute to our operational excellence, help maintain our technological capabilities and support our ability to serve the public cost effectively in an increasingly digital world.

Who this Policy applies to

This Policy applies to you if:

1. You work for, or represent, the BBC or one of its subsidiaries, and
2. You use BBC-provided technology as part of your role (hardware or software), or you use BBC credentials to access external websites or applications

This includes, but is not limited to:

- employees, full-time or part-time
- those on a fixed term or temporary contract
- freelancers, contractors or consultants
- volunteers or interns

The essential things you must do or not do

These high-level essential mandatory requirements are the most important for you to understand and follow to meet the Policy objectives.

Procurement

1. You must only procure and/or use BBC-authorised technology hardware, software and telephony. You must be able to justify why it is needed for your role and ensure it's authorised for your use case.

This includes, but is not limited to, laptops/desktops, software (both local or online), mobiles and services. Raise all technology requirements via the IT Requests catalogue. Requests are subject to meeting suitable business justifications and approval.

Authorised software includes - but is not limited to - physical, virtual, websites and installed and online applications. Software authorisation confirms compliance with terms and conditions of use. It also ensures data protection, information security, BBC brand, intellectual property, artificial intelligence and assistive technology have all been considered and controls identified.

Only Authorised Software can be installed on BBC devices or networks under the following conditions: - by IT specialists or those employees with express permission to install software, if appropriate licences are in place, if it will be used in accordance with the publisher's terms and conditions.

2. You must only use authorised routes to purchase non-standard technology hardware or software. You must have a valid business justification and written approval from your Finance Director and appropriate authoriser before raising a request. All software (new or renewal) must be on the Authorised Software List.

Do not purchase technology outside of approved suppliers or through expenses. All requests are reviewed and challenged if they do not meet the requirements for approval.

Non-standard technology refers to any hardware or software that is not part of the existing IT catalogue.

3. All software licenses must be procured and registered with the BBC as the owner using BBCSoftware.licensing@bbc.co.uk

Do not use your personal or corporate email address. This includes software being used on a device not connected to the BBC network. Doing so can invalidate the licence and your use of it.

4. You must ensure any technology procured or developed meets the BBCs accessibility requirements.

If you have a requirement for assistive technology these must be ordered via the specific AT request route. This includes both hardware and software purchased for wider consumption or on a one-off basis.

Responsible Use

5. You must act responsibly whenever using BBC credentials, systems or data, and only for BBC-related activities. You must NOT use these tools for personal or external freelance reasons in a way that interferes with your work or compromises the BBC and its systems.

This includes, but is not limited to, the use of laptops, mobiles, printers, websites, applications and software. Limit the use of BBC systems and devices for personal reasons.

For example, don't use BBC devices to call premium lines, make overseas personal calls or download non-work-related apps/software or illegal services.

Personal use that incurs charges to the BBC may be reimbursed via payroll.

Do not use BBC credentials, including email, for registration of personal accounts or access to applications or services that are not on the authorised software list.

6. You must install the latest security patches and updates (including software) on your BBC or personal enrolled devices as soon as they become available. Where a device can no longer be updated it must not be used.

It is important to maintain the latest updates for your laptop, mobile or applications. This ensures optimal performance and reduces the risk of technical issues and/or security breaches.

7. You must check that all technology you are using, or responsible for, is assigned to you correctly. All BBC-provided mobile devices must be registered using BBC Essentials.

To ensure accurate tracking and billing of BBC provisioned technology it is important to ensure you check what is assigned to you. This includes managing shared or group devices used through non-human accounts. Anything no longer required is removed through formal processes.

Registering your BBC device keeps it secured and encrypted and enables access to BBC apps

Data Management, Security and Handling

8. You must only use BBC-approved methods and services for accessing, storing, sharing and viewing data when working remotely or in BBC premises.

This ensures proper backup and access control to BBC data as well as preventing leaking of sensitive information in the event the device is lost or stolen. Store information appropriately according to its sensitivity.

Do not use personal file-sharing services for BBC data or store personal files in BBC storage solutions.

You also need to ensure you are aware of your surroundings when viewing or discussing sensitive information and take mitigating actions to prevent leaking of sensitive information.

9. You must take due care and responsibly store all BBC technology provided to you. Any devices that are faulty/damaged, lost or stolen need to be reported immediately to your IT service provider.

Any user damage to BBC devices is chargeable to your BBC charge code. The cost may be recovered from you depending on the circumstances or damage caused.

Do not leave technology assets unattended or in a situation which makes them likely to be stolen.

In the event of theft, it is your responsibility to raise a police incident report and contact the IT service provider, which will lock lost or stolen devices out of the BBC network.

10. You must return all BBC technology devices and cancel software licenses when no longer needed.

Before you leave the BBC, agree a date with your line manager to return all BBC technology assigned to you, cancel SIM cards, phone extensions, software subscriptions etc.

You are also responsible for wiping data/ resetting mobile devices before handing them back as these may be reassigned to other employees.

Non-Corporate Communication Channels (NCCs)

In general, you are expected to use formal approved BBC communication channels and systems for BBC business.

11. If you use a Non-Corporate Communication Channel (NCCC) for BBC business, you must transfer all key discussions, decisions and information to an approved corporate system as soon as possible.

Using NCCCs for significant BBC business means you're responsible for making sure the information is properly recorded, as BBC have recordkeeping responsibilities, and it can lead to compliance risks if you don't. See the Records Management Corporate Policy for more detail.

12. If asked, you must be able to search and provide all relevant information from any NCCC you have used for BBC business.

BBC information held in NCCCs is subject to the Freedom of Information Act (FOIA) and the Data Protection Act if it relates to official BBC business.

NCCs include private accounts on private devices.

Requests may come from, for example, a FOIA request, Subject Access Request, audit, corporate investigation, or legal proceeding.

Recording and transcribing calls

13. You must only record or transcribe calls or meetings when there is a legitimate business need, all participants have provided prior consent, and no prohibited circumstances apply.