Topics > Business Procedures > Data Protection: Model Policies

# Bring Your Own Device (BYOD) Policy

## Policy Statement

[Organisation] allows employees to bring their own device (eg smartphone, tablet, laptop) into the workplace, and to use the device to access company data and information.

This policy sets out the terms relating to the use of personal devices in the workplace.

## Scope of the Policy

Employees are allowed to bring their own devices into the workplace, and to use those devices to access company data and information. This is subject to the points below.

1. The device must be checked by the IT department to ensure that there are no security risks before it is used to access company data and information.
2. The device must have virus protection installed. This must be the protection that is defined by the IT department.
3. Any software on the device that will be used to access company information must be checked by IT and configured by them.
4. Only the following browsers can be used when accessing company information [specify browsers].
5. Only devices of the following brand are covered by this policy.
6. This policy specifically applies to [laptops/smartphones/tablets/other]. Employees are not allowed to bring [laptops/smartphones/tablets/others] into the workplace and use them to access company information.

## Security

The security of company information and data is paramount. Employees must not do anything which might compromise that security when using their own devices.

1. The device must be password protected. The employee should not share the password with anyone without their line manager’s knowledge and permission.
2. All passwords should be a mix of numbers and letters, and must be replaced every month.
3. The device should lock after it has been left unattended for more than five minutes.
4. The device should not be used to access company data or information in a public place where non-employees might be able to see the content.
5. The employee should never use the device to access company data over an unsecured network.
6. The employee should ensure that there is a regular back up of any company material that is placed on the device.
7. If the device is lost or stolen, the employee must inform the line manager immediately and always within 24 hours. It might be necessary for the IT department to remotely wipe the device clean. If this does happen there is no guarantee that personal information will not be deleted.
8. If the device has a camera or video function, this must never be used in the workplace without the express permission of the employee’s line manager and all the individuals who are being filmed.
9. When a device is no longer being used, all company data and information must be deleted from the device. The IT department should be asked to check that this has been carried out thoroughly.
10. The following company data and information must never be accessed from a personal device [list any information that must not be accessed, such as employee’s personnel files].
11. The following apps may not be downloaded onto a device that is being used for company business [list apps].
12. Personal data relating to other employees must never be stored on a personal device.

## Personal Use in the Workplace

Although it is acknowledged that the device is the employee’s personal property, employees must not spend time at work using the device for personal reasons. During working hours, the device should only be used for company purposes.

1. The personal device can be used for personal purposes during any designated breaks.
2. A device that is only used for personal purposes must never be used to connect to the organisation’s network.
3. The following websites are blocked by the organisation and must not be accessed by an employee during working hours [list websites].
4. Any personal device which is used for company purposes must never (during or outside working time) be used to access pornography or any illicit or illegal material.
5. Personal calls should only be taken during working hours when the matter is urgent or an emergency.
6. Unless the device has a hands-free facility it should never be used when driving.

## Cost of the Device

The device is the employee’s property and remains the property of the employee at all times.

1. The organisation [will/will not] make a contribution to the cost of the device. [If a contribution is to be made explain how this will be calculated.]
2. The organisation will refund the cost of any phone calls made for work purposes on receipt of an itemised bill.
3. If the employee is working away from the office and is required to pay for Wi-Fi access, the organisation [will/will not] refund the cost.
4. If the employee is a homeworker, the organisation [will/will not] make a contribution to the cost of [Wi-Fi/phone line/other — if this cost is to be met explain how it will be calculated].
5. If the employee is working outside of the UK, the cost of [explain what] will be refunded.

## Leaving the Organisation

When an employee leaves the organisation, he or she must ensure that any company information has been removed from the device.

1. The device should be taken to the IT department who will check the device to ensure that all company information has been removed.
2. The employee should advise any customer, client or other contact of the organisation who has been given a phone number relating to a personal device that he or she is leaving the organisation. The individual should be given a contact number of another employee. The employee should inform their line manager of all individuals who have been contacted for this reason.

## Breach of this Policy

Any breach of this policy could lead to disciplinary action being taken against the employee concerned.

|  |  |
| --- | --- |
| Signed: | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| Date: | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| Policy review date: | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |