Changes made to the attached policy (November 2024)

1. The policy has been significantly revised and restructured. This work was completed by the Director of IT Services.

2. Consistency has been imposed so that capital letters and hyphenation are more consistent; bullet point lists have been reformatted.

3. A contents page has been added and updated.

4. Inclusive language has been used.

5. Language has been updated to reflect the organisation of the Trust Board (rather than the previous Governing Body). It is also designed to reflect the multi-school nature of an academy trust.

The NSB Trust

Bring your own device (Staff) Policy

To be reviewed annually

Contents

1. Introduction 4
1. Acceptable use 4
3. Non-acceptable use 5
4. Devices and support 5
5. Security 5
Appendix A. Printable disclaimer for staff wishing to use their own device 6

1. Introduction

The Trust has implemented this policy to protect the Trust and all parties when using ICT and media devices. Staff are able to use devices at work and outside of work for work related activities provided the terms of this policy are met. The Trust reserves the right to revoke this privilege if users do not abide by the policies and procedures outlined below.

This policy is intended to protect the security and integrity of the Trust's data and technology infrastructure. Limited exceptions to the policy may occur due to variations in devices and platforms. This policy is not designed to offer protection for the device itself. The safety of the user's own device is the responsibility of the user.

Mobile devices within the context of this policy includes any mobile phone, tablet, laptop, MP3/iPod or other device which is capable of connecting with the internet or mobile networks or taking image or sound recordings.

This guidance is in addition to the Trust's Acceptable Use Policy.

1. Acceptable use

The Trust embrace the use of new and mobile technologies and acknowledge they are a valuable resource in the classroom having educational purpose.

However, by accessing the Trust's systems and networks, it is likely that staff will use personal data and so must abide by the terms of the Data Protection Act (2018) when doing so (including ensuring adequate security of that personal information).

All employees must agree to the following terms and conditions in order to be able to connect their devices to the company network:

- All staff who wish to use their own devices to access the Trust's networks must sign and return the statement at the conclusion of this policy
- When in Trust locations, staff should connect their device via the Trust's wireless BYOD network for security
- When out of Trust locations, staff should access work systems on their mobile device using the Office 365 web portal only
- All internet access via the network is logged and as set out in the Acceptable Use policy, employees are blocked from accessing certain websites whilst connected to the Trust networks
- The use of camera, microphone and/or video capabilities are prohibited whilst in Trust locations unless this has been approved by The Director of Information Services. If approved, any pictures, videos or sound recordings can only be used for Trust purposes and cannot be posted or uploaded to any website or system outside of the Trust networks
- You must not use your device to take pictures/video/recordings of other individuals without their advance written permission to do so
- WhatsApp must not be used on personal devices for Trust related communication. Members of staff are able to use WhatsApp on their own devices for personal communication. However, staff should not communicate internally with other staff members for Trust business using their personal WhatsApp accounts, sharing Trust related information which could include categories of personal data

3. Non-acceptable use

Any apps or software which are downloaded onto the user's device whilst using the Trust's own networks is done at the user's risk and not with the approval of the Trust.

Devices may not be used at any time to:

- store or transmit illicit materials
- store or transmit proprietary information belonging to the Trust
- harass others
- act in any way against the Trust's Acceptable Use policy and other safeguarding and data related policies
- technical support is not provided by the Trust on the user's own devices

4. Devices and support

Smartphones including iPhones and Android phones are allowed.

Tablets including iPad and Android are allowed.

Devices must only use the BYOD wireless network.

In order to prevent unauthorised access, devices must be password/pin/fingerprint protected using the features of the device and a strong password is required to access Trust networks.

5. Security

When using personal data, it is the user's responsibility to ensure they keep data secure on their device. This includes preventing theft and loss of data (for example, through password protection and cloud back up), keeping information confidential (for example, by ensuring access to emails or sensitive information is password protected) and maintaining that information.

The Trust does not accept responsibility for any loss or damage to the user's device when used on Trust's premises. It is up to the user to ensure they have their own protection on their own device (such as insurance).

Staff are advised not to use email apps which allow direct access to Trust emails without use of a login/password on personal devices.

If information is particularly sensitive, then users should ensure that the data is either appropriately secured or deleted from the device (including from any local copies which may have been stored on the device.

In the event of any loss or theft of personal data, this must be reported immediately as a data breach in accordance with the Trust's Data Breach policy.

The Trust may require access to a device when investigating policy breaches (for example, to investigate cyber bullying).

Staff are not permitted to share access details to the Trust's network or Wi-Fi password with anyone else.

Appendix A. Printable disclaimer for staff wishing to use their own device

Disclaimer

The Trust will not monitor the content of the user's own device but will monitor any traffic over Trust systems to prevent threats to the Trust's network.

The Trust reserves the right to disconnect devices or disable services without notification.

The employee is expected to use the devices in an ethical manner at all times and adhere to the Trust's policy as outlined above.

The employee is personally liable for all costs associated with the device.

The Trust reserves the right to take appropriate disciplinary action up to and including summary dismissal for non-compliance with this policy.

I confirm that I have read, understood and will comply with the terms of the Bring Your Own Device Policy when using my mobile device to access the Trust's networks.

Signed: ……

Date: …….

Print Name: …….