Policy:	Bring Your Own Device
Person(s) responsible for updating the policy:	Chief Executive Officer
Date Approved:	Board of Directors on 7 July 2016
Date of Review:	Every 3 years
Status:	Non statutory

Tudor Park Education Trust oversees this policy but the local governing body of each academy or school within the Trust is responsible for the implementation of the policy.

This policy should be read in conjunction with the government document *'Bring your own device guidance'* available at www.gov.uk/government/collections/bring-your-own-device-guidance#other- and the Information Commissioner's document *'Bring your own device (BYOD)'* available at ico.org.uk/news/latest_news/2013/~/media/documents/library/Data_Protection/Practical_application/ico_bring_your_own_device_byod_guidance.pdf.

This policy should be read in conjunction with other ICT related policies:

- Data protection.
- Use of ICT and the internet by staff (useful for legal references).
- Management and retention of records.
- Secure data handling.
- Social media.
- Staff email.

Background

ICT is a vital tool in the administration of the school. Increasingly, teachers and support staff are able to use their own personal devices, as well as the network of devices owned by the school, to support their work. This trend is known as 'Bring your own device' (BYOD) and involves the use of mobile devices such as smart phones, laptops and tablets.

Teachers and support staff need to be aware of what is acceptable to the school when using their own devices, particularly when dealing with confidential matters and any data which is covered by the Data Protection Act 1998.

Introduction

This policy is in place for the occasions when staff use their own ICT equipment when dealing with data belonging to the school.

There is a network of computers available for use by pupils and staff. All pupils and staff have a login name, password and an email account.

The email system is available for use both from within the school and externally.

The school is responsible for ensuring that the school infrastructure/network is as safe and secure as is reasonably possible and that:

- Users can only access data to which they have right of access.
- No user should be able to access another's files without permission (or as allowed for monitoring purposes within the school's policies).
- Access to personal data is securely controlled in line with the school's personal data policy.
- Logs are maintained of access by users and of their actions while users of the system.

When staff use their own devices (eg laptops, tablets, smartphones) it is imperative that:

- The protocols already in use are maintained.
- No vulnerabilities are introduced into the school's existing secure environments.
- Data protection matters are complied with.

Any queries regarding this policy should be addressed to the Principal.

Objectives and targets

The objective of this policy is to develop an appropriate code of practice for the use of ICT by staff at Feltham Community College when using their own devices (BYOD).

Action plan

The following code of practice must be adhered to by staff using BYODs to carry out their work.

All staff are expected to have read, understood and abide by the following school policies:

- Data protection.
- Use of ICT and the internet by staff (useful for legal references).
- Management and retention of records.
- ICT: Social media.
- ICT: Email.

- ICT: Could Usage.
- ICT: Use of the Internet and Intranet by Staff.

They are also expected to sign the ICT: Staff acceptable BYOD usage agreement – see appendix 1 – to ensure that they understand their responsibilities.

They will also have signed the ICT: Staff acceptable usage agreement.

Staff who receive a laptop which is the property of the school will also be expected to sign the ICT: Staff acceptable laptop usage agreement.

All BYODs must have appropriate security in place and it must be updated regularly. For instance you should ensure that your device is password protected and has adequate virus protection. It is the staff member's responsibility to ensure this.

Handling personal data (where Data Protection Act 1998 applies)

Sensitive information relating to the school must not be transferred to any BYOD. This is to prevent personal data relating to school matters being accidentally or deliberately compromised or accessed by anyone other than the member of staff. This also applies wherever data is stored (eg on the device, portable hard drive, memory card, SD card, intranet or cloud). Such data may include:

- Information relating to staff, eg performance reviews.
- Pupil reports.
- SEN records.
- Letters to parents.
- Class-based assessments.
- Exam results.
- Whole school data.
- Medical information.

Members of staff should speak to the network manager about whether an encrypted channel (eg VPN or HTTPS) could be set up to offer better security when transferring data of a secure nature from a BYOD to the school's network. Similarly, before using BYODs in cafes, hotels etc staff should seek advice from the network manager about the safety of such operations.

Handling other data relevant to the school

Where a BYOD is used for work purposes that do not involve personal data, for example accessing email on smart phones, (and therefore have data protection implications) it is appropriate to maintain a clear separation of the work on the device from work which is of a confidential nature.

It is still important that school-related non-sensitive data held on BYODs must be accessible only by a password, PIN or encryption. This is to prevent data relating to school matters

being accidentally or deliberately compromised or accessed by anyone other than the member of staff.

It is essential to be careful when installing any third-party software onto a BYOD. Untrusted sources have the potential to contain malware which could compromise any personal material belonging to the school. If in doubt, consult the network manager before uploading.

Connecting BYOD to the School Network

All staff and visitors are permitted to connect to the schools Guest Wireless Network. This will give internet access to most websites. All access to this network is logged. Access to the network via a physical connection (Ethernet cable) is strictly prohibited.

Monitoring and evaluation

The policy will be monitored and evaluated regularly taking into account any incidents which occur or technological developments which might need a change in the policy.

Reviewing

The efficacy of the policy will be discussed annually as part of the governors' rolling programme of reviews.

Next school review due: July 2019

APPENDIX 1

ICT: Staff acceptable BYOD usage agreement

I understand that anyone other than myself must never have access to any sensitive data held on the BYOD.

I understand that I am responsible for the safety of sensitive school data that I use or access.

If I am in any doubt as to the sensitivity of data I am using, I will refer to the school's secure data handling policy, and to the Principal (in the role of data controller under the Data Protection Act 1998) if still unsure.

I will always adhere to copyright.

I will always log off the system when I have finished working.

I will only access the school's systems with my own name and registered password.

Passwords that I use to access school systems will be kept secure and secret.

If I have reason to believe my password is no longer secure, I will change it immediately. I will inform the network manager as soon as possible so that any access with my old password can be monitored and appropriate action taken.

When I leave the school's employment, all data relating to the school will be returned to the school.

I understand that when in school and not being used, the BYOD must be kept in an office, locked room or drawer. It must not be left in an unlocked, unattended classroom.

I understand that, whenever possible, the BYOD must not be left in an unattended car. If there is a need to do so, it will be locked in the boot.

I will check that the BYOD is covered by my normal household insurance, whether in England or abroad.

I understand that when being transported, the carrying case supplied must be used at all times.

I understand that I have the responsibility to ensure the virus protection software that has been installed is kept up-to-date. I also understand that I must *always* follow the virus protection procedures as directed by the school's network manager to ensure virus protection is always kept up-to-date.

I will follow the guidance provided by ICT support staff to ensure the anti-virus protection on my BYOD is kept up-to-date.

If I use removable media I will ensure that this has been carefully checked to ensure it is free from any type of virus.

I understand that I may load software onto the BYOD but it must:

Be fully licensed.

Not corrupt any software or systems already installed on the BYOD.

Not affect the integrity of the school networks when connected to either the curriculum or administration networks.

I will check with the network manager/technician should I need to install additional software.

I will always adhere to the following associated school policies:

- Data protection
- E-safety (useful for legal references)
- Management and retention of records
- Secure data handling
- Social media
- Staff email
- Staff professional identity protection.

I understand that the school may monitor my BYOD activity.

I understand that activity that threatens the integrity of the school ICT systems, or activity that attacks or corrupts other systems, is forbidden.

In order to maintain the security of data, I will take the following steps:

I will store data only for as long as is necessary for me to carry out my professional duties.

If I need to transfer data files, I will only do so using encryption as advised by the network manager.

I will not use email to transfer data files but save them to the school network area if other staff need access to the information.

I understand that if I do not adhere to these rules outlined in this agreement, my privilege of working with the BYOD could be suspended and other disciplinary consequences may follow, including notification to professional bodies, where appropriate.

If an incident is considered to be an offence under the Computer Misuse Act or the Data Protection Act this may require investigation by the police and could be recorded on any future criminal record checks.

Name _____

School / Academy _____

Date _____