QUEEN ELIZABETH'S SCHOOL (WIMBORNE MINSTER)

Home & Mobile Working (HMW) & Bring Your Own Device (BYOD) Policy

Title of Policy	Home & Mobile Working (HMW) & Bring Your Own Device (BYOD) - Policy
Policy Type	School
Review Cycle	3 Years
Policy prepared by	Stephen Jones, COO
Committee responsible	Community and Environment
Date of review by committee	9th November 2017
Date of approval or submission to FGB	21st November 2017
Next Review	November 2020

1. Introduction

This policy is in place for the occasions when staff, students or visitors use their own electronic devices either within the school or when working remotely away from the school. These concepts are usually known as Bring Your Own Device – (BYOD) or Home and Mobile working (HMW).

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 (e.g. 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.

To provide assurance that safety and security is being maintains the school hold Cyber Security Essentials certification which is externally assesses annually.

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

2. Objectives and targets

The objective of this policy is to develop an appropriate code of practice for the use of ICT by Staff, Students and Visitors at Queen Elizabeth's School when undertaking Home and Mobile working (HMW) or using their own devices (BYOD).

3. Legal Requirements

- Computer Misuse Act – 1990
- Data Protection Act – 1998
- Malicious Communications Act 1988
- http://www.bris.ac.uk/media-library/sites/infosec/documents/guide.pdf

4. Responsibilities and Practices

4.1 Home and Mobile Working (HMW)

The following code of practice must be adhered to by all staff undertaking Home and Mobile working. All are expected to have read, understood and abide by the policies and references listed in section 5, which is included in the relevant section of the staff handbook.

Mobile working and remote system access offers great business benefits but exposes new risks that need to be managed. QES has established risk based policies and procedures that support mobile working or remote access to systems that are applicable to users, as well as service providers.

Risks

Mobile working and remote access extends the transit and storage of information (or operation of systems) outside of the corporate infrastructure, typically over the Internet. Mobile devices will also typically be used in spaces that are subject to additional risks such as oversight of screens, or the theft/loss of devices. Organisations that do not establish sound mobile working and remote access practices might be vulnerable to the following risks:

4. Responsibilities and Practices

4.1 Home and Mobile Working (HMW)

- **Loss or theft of the device:** Mobile devices are highly vulnerable to being lost or stolen, potentially offering access to sensitive information or systems. They are often used in open view in locations that cannot offer the same level of physical security as your own premises.
- **Being overlooked:** Some users will have to work in public open spaces, such as on public transport, where they are vulnerable to being observed when working. This can potentially compromise sensitive information or authentication credentials.
- **Loss of credentials:** If user credentials (such as username, password, or token) are stored with a device used for remote working or remote access and it is lost or stolen, the attacker could use those credentials to compromise services or information stored on (or accessible from) that device.
- **Tampering:** An attacker may attempt to subvert the security controls on the device through the insertion of malicious software or hardware if the device is left unattended. This may allow them to monitor all user activity on the device, including authentication credentials.

Risk Management

Educate users and maintain awareness: All users should be trained by the school ICT Unit on the use of their mobile device for the locations they will be working in. Users should be supported to look after their mobile device and operate securely by following clear procedures. This should include direction on:

- secure storage and management of user credentials
- incident reporting
- environmental awareness (the risks from being overlooked, etc.)

Apply the secure baseline build: Develop and apply a secure baseline build and configuration for all types of mobile device used by the organisation.

Vendor Updates and App Patches: Mobile devices inc BYOD must be kept up to date.

Protect data at rest: Minimise the amount of information stored on a mobile device to only that which is needed to fulfil the business activity that is being delivered outside the normal office environment. If the device supports it, encrypt the data at rest.

Protect data in transit: If the user is working remotely the connection back to the school network will probably use the Internet. Users should only use the schools provided remote working solution which is encrypted. Email is not encrypted and should not be used for the transfer of sensitive data.

4.2 Bring Your Own Device (BOYD)

The following code of practice must be adhered to by staff, students & visitors using BYODs to carry out their work. All are expected to have read, understood and abide by the policies and references listed in section 5.

Staff, Students and Governors are expected to sign the ***BYOD – Responsible user agreement*** – see appendix 1 – to ensure that they understand their responsibilities.

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.

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 (e.g. on the device, portable hard drive, memory card, SD card, intranet or cloud). Such data may include:

- Information relating to staff, e.g. 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 IT Systems Manager about security when transferring data from a BYOD to the school's network. Similarly, before using BYODs in cafes, hotels etc staff should seek advice from the ICT manager about the safety of such operations.

Handling other data relevant to the school

Where a BYOD is used for work purposes that does not involve personal data, for example accessing email on smart phones, (and therefore have data protection implications) it is important to maintain a clear separation of this data from any personal data on the BYOD.

It is also 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 IT Systems Manager before installing.

Connecting BYOD to the School Network

All staff, students and visitors are permitted to connect to the schools SWGuest Wireless Network. This will give filtered internet access. All access to this network is logged against the user's name. 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

5. Link and References

- Cyber Security Standards
- Acceptable use of ICT Facilities (Staff, Students & Visitors)
- Password Standards
- Social Media Policy
- E – Safety Policy
- Behaviour Policy

Appendix 1 – BYOD - Responsible User Agreement – Staff, Students & Governors

Introduction

Queen Elizabeth's School and its staff are committed to providing you with the opportunities to fulfil your potential, enhance your learning experiences and develop life skills and knowledge which will support you in the years beyond secondary school.

At Queen Elizabeth's school, we provide the facility for pupils to access our wireless network using their own smart phones, tablets and other mobile devices, for the purpose of supporting individual and collaborative learning and at certain times, for social use.

Queen Elizabeth's school's wireless network is an additional tool to support pupil learning and it should not be regarded as compulsory to bring a device. If a teacher requires pupils to use the wireless network but the pupil has not brought their own device, devices will be supplied by the school for that lesson.

All Staff, Students & Governors must take full responsibility for their conduct when using mobile devices, and when accessing the school's wireless network and its facilities.
Before you can bring and utilise your own mobile device in school, and access the WIFI, you must:

- Read this policy thoroughly
- Ask your parent/carer to read the Agreement

By bringing your device to use in school, you are committing yourself to following Queen Elizabeth's school's BYOD policy and procedures.

Please carefully read the rules and procedures on the following page.

Stephen Jones
Chief Operating Officer

Responsible User Agreement – Declaration and Agreement

1. I will be responsible for the care, safety and use of my mobile device at all times. This includes my journey to and from school and when on the school premises.

2. Students: I will only use my device for learning activities approved by my teacher and ensure that my device will be clearly visible on my desk so that my teacher can monitor it. Staff/Governors: I will only use my device for activities related to school business.

3. I agree not to access materials which will put strain on the network and could limit internet access for other users.

4. I will be responsible for any use of my 3G/4G network / use of my personal data allowance; I understand that the school cannot be responsible for monitoring my use of my 3G/4G, nor is it responsible for any costs / penalties for excess use incurred.

5. I will advise an appropriate ICT member of staff if I find a page, message or pictures which are inappropriate.

6. I will not communicate with others using threatening, rude or swear words or in ways which are inappropriate.

7. I will remember that electronic mail (e mail), online messaging and website posts are not guaranteed to be private.

8. I will ensure my device speaker volume is at an acceptable level.

9. I will not respond to, or initiate, any text message or call when in class or school meetings.

10. I will only take or post pictures, personal information or videos of me or others, with the consent of staff, students or governors involved.

11. I accept that the school is not responsible should my device be lost, broken or stolen.

12. I accept that if I do not follow the Responsible Use Agreement, the school will withdraw the right for me to use my mobile device.

Consequences of Inappropriate Use

Failure to comply with the Responsible Use Agreement will result in one or more of the following actions being taken:

- Your device confiscated and stored securely until the end of the school day.
- Your parent/carer/*Line Manager* will be contacted to inform them of the rules you have breached.
- Your access to the school network and online facilities will be withdrawn on either a temporary or permanent basis.
- Your future use of the school's ICT facilities will be restricted.
- Any other action deemed appropriate by the Head teacher will be taken.

Signed & Date

_____ Date:_____