Date Reviewed	May 2023
Review Date	May 2024

Agreed by: Learning and Achievement Committee Date: 18/05/23

Name: Sally Evans Signature: 

BRING YOUR OWN DEVICE POLICY (BYOD)
(GDPR Compliant)

This policy applies to employees who use their own personal devices such as laptops, tablets or mobile phones for work purposes.

This policy outlines how employees should ensure that they protect any personal data while using their own devices for work purposes along with protecting School data. This policy should be read in conjunction with the School's Data Protection Policy and the Social Media Policy.

Data Protection Officer

The Data Protection Officer is responsible for the implementation of this policy. All enquiries about data protection should be directed to the appointed Data Protection Officer.

Data Protection Legislation

The General Data Protection Regulation (GDPR) requires the School to process any personal data in accordance with the data protection principles. "Processing" includes obtaining personal information, retaining and using it, allowing it to be accessed, disclosing it and, finally, disposing of it. The School must ensure that personal data is protected by appropriate confidentiality, technical and organisational measures against unauthorised or unlawful processing or disclosure, and against accidental loss, damage or destruction.

Employees who wish to use their own device for work-related purposes should contact the Headteacher in the first instance in writing with the name and model of the device and the purpose for which it is intended to be used. The School has a list of devices that it has assessed as providing the appropriate level of security for the processing of personal data, which can be obtained from the Data Protection Officer. Smart phones and tablets that are not on the School's list of approved devices are not allowed to connect to the Network. Any Rooted (Android) or Jailbroken (IOS) devices are strictly forbidden from accessing the School network.

Under no circumstances should an employee use their own device without prior consent and authorisation from the Line Manager.

Sensitive personal data

"Sensitive personal data" is information about an individual's:

- Racial or ethnic origin;
- Political opinions;
- Religious beliefs or other beliefs of a similar nature;
- Trade union membership (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992);
- Physical or mental health or condition;
- Sex life;
- Commission or alleged commission of any criminal offence; and
- Proceedings for any offence committed or alleged to have been committed, the disposal of such proceedings, or the sentence of any court in such proceedings.

Employees must not process any sensitive personal data on a personal device. Employees should check whether any sensitive personal data has passed to their personal devices by whatever means. If an employee discovers any sensitive personal data on their device, they must notify their manager immediately and arrange for its permanent deletion from the device.

Employees' obligations regarding BYOD

Security

Before using their own device for work-related purposes, employees must ensure that they use a strong password of at least 6 characters and a combination of upper and lower-case letters and symbols to lock their device or a biometric access control. The device must be capable of locking automatically after being left idle for a set time of no more than 5 minutes, deleting data automatically or becoming inactive if an incorrect password is entered after five attempts. Employees must confirm to the School what data might be deleted automatically.

In addition, employees must:

- Use encryption software on their devices to store personal data securely;
- Ensure that if they transfer data (either by email or by other means), they do so via an encrypted channel (for example a VPN or HTTPS for individual services);
- Ensure that they assess the security of any open network or Wi-Fi connection (employees should not use unsecured Wi-Fi networks under any circumstances);
- Not download unverified or untrusted apps that may pose a threat to the security of the information held on their devices;
- Not, under any circumstances, use corporate personal information for any purpose other than for their work and as directed or instructed by the School;
- Use different applications for business and personal use;
- Ensure that they have a system of software in place for quickly and effectively revoking access that a user might gain to a device in the event of loss or theft;
- Make sure that any software that they use is genuine software installed under an appropriate licence agreement between the employee and the relevant manufacturer to prevent any security vulnerabilities; and
- Report the loss or theft of a device used for work-related activities immediately to the Data Protection Officer.
- Ensure approved anti-virus software is used, including the latest security updates to the operating system.
- Home Wi-Fi networks must be encrypted, and caution must be exercised when using any public Wi-Fi.

Employees are permitted to access any document on the School's network/private cloud. Employees must always log out of the School's server/network/private cloud between sessions.

Employees must not copy data from approved devices to other personally owned devices unless in cases of emergency or with the approval of the Employer.

Employees must not use public cloud-based sharing or public back-up services without prior authorisation from the School.

An employee is not permitted to download or access certain applications or types of data that require the identification of the employee's location or an additional level of authentication.

Mobile-device management

An employee must ensure that their device is subject to mobile-device management so that if the device is stolen, upgraded, recycled for money or given to family or friends, the employee is able to locate the device remotely and delete data on demand. The employee must limit the purpose of mobile-device management to the detection of the device and the remote deletion of data. If the device is stolen, the employee must be able effectively to wipe any confidential data on the device immediately by way of a remote "locate and wipe" facility.
Any lost or stolen device must be reported to the School within 24 hours.

Technical support

If employees require any technical support with their devices, they should ensure that the third party providing such support only has access to data as is necessary to complete their work and the data must not be transferred to a third-party device unless there is no other way of rectifying the technical problem. If data is transferred to a third-party device, the third party must warrant, and the employee must ensure, that the information is removed permanently from such third-party device once the problem has been rectified.

Retention of personal data

Employees must not retain personal data for longer than is necessary unless there is a requirement to do so to comply with any legal obligation. In any event employees should confirm with the Data Protection Officer what is and is not an acceptable period to retain personal data.

Deletion of personal data

Employees must ensure that any information they delete is deleted permanently and not left in the device's waste-management system. An employee may need to use overwriting software to achieve this. Where the information is stored or categorised with other information that is still live it may not be practical to do this. In these circumstances, it is sufficient for the employee to put the information "beyond use". This means that the employee must:

- Ensure that he/she does not use the personal information to make any decision that affects an individual or in a manner that affects an individual in any way;
- Not give any other organisation access to the personal data in any way;
- Surround the personal data with appropriate technical and organisational security; and
- Commit to the permanent deletion of the information when this becomes possible.

If an employee uses removable media, for example a USB drive or CD, to transfer personal data, they must ensure that the personal data is deleted once the transfer is complete.

Third-party use of device

Employees must ensure that if family or friends use their devices, they are unable to gain access to any information that is work-related. The Data Protection Officer can guide you on how to protect this information.

Termination of employment

When an employee leaves the School, they must delete all work-related personal data on their own device prior to their last day with the School. The Data Protection Officer will check the devices to ensure the deletion is complete.

Monitoring

As part of the on-going obligations under GDPR, the School will monitor data protection compliance in general and compliance with this policy. Before undertaking any such monitoring exercise, the School will outline the purpose for the monitoring and the specific benefits of this.

All employees should be aware, that whether through IT policies or employment contracts, the School reserves the right to access personally-owned devices for the purpose of ensuring the effectiveness of this policy, in the event of termination or a suspected breach of this policy.

Consequences of non-compliance

If an employee is suspected of breaching this policy, the School will investigate the matter in line with the disciplinary procedure. If any breaches are established, this could result in disciplinary action up to and including dismissal. An employee may also incur personal criminal liability for breaching this policy.

Review of procedures and training

The School will provide training to employees on data protection matters on a regular basis.

The School will review and ensure compliance with this policy at regular intervals.

The employee assumes full liability for risks including but not limited to, the partial or complete loss of personal information due to an operating system crash, errors, bugs, viruses or malware.

Employees must agree to the terms and conditions set forth in this policy in order to be able to connect the devices to the School Network.