Westbrook Hay Prep School

DATA ENCRYPTION POLICY

Westbrook Hay Prep School takes its responsibility for obtaining, using and storing data seriously. As such it wishes to ensure that all data held by the school electronically is adequately protected from loss and inappropriate access, whether by accident or theft. Furthermore, under the Data Protection Act 1998, Westbrook Hay Prep School is required to have in place appropriate policies and procedures which ensure the secure storage of data covered by the 'Act' at all times.

To reduce the risk of unauthorised access to data held by the school on electronic and mobile devices Westbrook Hay Prep School has established a comprehensive policy of data encryption. This covers data which can be accessed from outside the school and which can be removed from the school.

This policy covers data stored by the following means:

- Laptops
- Handheld portable devices such as mobile phones, PDAs and Tablet devices
- Portable storage devices such as USB data sticks, external drives
- Removable media such as DVDs, CDs, floppy disks etc

IMPLEMENTATION

Encryption will be applied to relevant files on all static PCs located at Westbrook Hay Prep School's premises, in order that data stored on these computers will be automatically encrypted. Users of these PCs will not be asked to supply a specific password for individual documents or files (unless there is a specific need for a document to be password protected/encrypted) once they have logged into their PC.

Access to the School's MIS (management information system), SchoolBase, will require a separate user name and password. Staff are advised that this password be changed on a regular basis and that it is different from their network password

The default encryption applied above will also apply to laptops owned by Westbrook Hay Prep School.

6-digit alphanumeric passcode will be used to encrypt handheld portable devices such as Tablet Devices. All devices will be managed by Westbrook Hay Prep School and Data Protection will be enabled. The school uses a cloud based solution, Meraki, to remote monitor these devices.

Portable storage devices such as USB data sticks will be encrypted before use with individual passwords in order that their portability is maintained. Westbrook Hay Prep School prohibits the use of non-encrypted data storage devices at all times; and has suspended the use of USB ports to ensure compliance with the policy.

Removable media such as CDs and DVDs drives will also be read only meaning they cannot be used to remove data.

Staff have access to a Westbrook Hay owned and managed Google Drive cloud storage account and use it as a means of moving & sharing documents. Google Drive should only contain documents that hold no personal data e.g. whole school timetables, policies and individual planning. Google Drive is excellent facility to quickly move photos from a secure portable device

to a secure network storage area. Staff are advised to remove photos from the Google Drive storage area as soon as is possible.

If a handheld device cannot be encrypted it must not be used to store person identifiable data. Furthermore, it must not be connected to any other of the Westbrook Hay Prep School's systems, whether by physical (e.g. USB) or wireless connection (e.g. Wi-Fi). The school runs a guest SSID identified as Westbrook Hay Guest to ensure no device can gain direct access.

Westbrook Hay Prep School aims to replace any devices which cannot be encrypted and which are capable of storing personal data where it is possible to do so.

COMPLIANCE

The encryption process will be managed jointly by the school's Head of IT and the IT Systems Manager. Passwords will be kept confidential by users and will adhere to the guidelines defined in the school's E-Safety policy. Passwords will be renewed on a 90-day basis.

Users will not remove or copy sensitive or personal data from Westbrook Hay Prep School's premises unless the data storage device is encrypted and is transported securely for storage in a secure location.

Staff are reminded that Emails should be treated as public property and therefore should contain as little personal data as is possible.

Users must protect all portable and mobile devices used to store and transmit personal information using approved encryption software.

Sensitive or personal data must be securely deleted when it is no longer required.

Non-compliant devices may be detected and disabled using management systems installed for this purpose without notice.

Users' privately owned mobile computing equipment or portable devices will not be permitted to connect to the school's network. [The one exception to this rule will be through remote desktop which is jointly monitored by the school's Head of IT and the IT Systems Manager.

Users will not publish any documents containing personal data on externally accessible websites.

Users must securely delete sensitive or personal information from their systems once it is no longer required.

Regular monitoring checks will be undertaken to ensure compliance with the criteria set out above.

All incidents resulting in a breach of these guidelines must be reported to the Headmaster.

According to ICO regulations, the Headmaster will inform the ICO if there are any losses of personal data.

Reviewer: Andy Lloyd, Head of IT
Review: 27.03.17
Review: Annually