The Westminster School

Portable Technology Agreement

The purpose of this agreement is to set out the criteria for the conditions relating to the use of **School owned** laptop computers. For the purpose of this agreement the term "laptop" is used to describe any portable computer device including laptops, notebooks, tablet PCs, cameras, flash drives, on which school data may be stored. Staff using such devices will be asked annually to sign to say they have read and understand the information in this agreement.

Your laptop is a valuable asset and an essential business tool. It needs to be protected, as does the information it stores. The data protection and information security policy govern the storage of data and personal information of devices and as such they should be read in conjunction with this. By following the simple security measures listed below, you can help protect yourself and your laptop.

Teacher/ Staff Responsibilities

Teachers/ members of staff must take personal responsibility for the security of the equipment, software and data in their care and abide by the following: (Please see glossary for definitions)

- Laptops in cars must be stored out of sight (e.g. in covered boot). Laptops should never be left in a vehicle for prolonged periods of time or overnight. If left the vehicle contents insurance must cover the cost in the event of theft.
- When travelling, laptops should not be left unattended in public places.
- Remain particularly vigilant when using your laptop and try to refrain from using it in public places (e.g. library, railway station).
- Your home contents insurance must cover the school laptop in the event of theft from your property.
- Although the laptop will be covered by the school's insurance policy you must take responsible measures to safeguard the resource. Always lock your laptop away in a cupboard or desk when it is not in use in school.
- Take all reasonable steps to ensure that the laptop is not damaged through misuse.
- Unauthorised or unlicensed software must not be loaded on to the laptop.
- Ensure the laptop is not used by unauthorised persons.
- Do not allow pupils to use your laptop unless it is part of a specific learning activity where they are closely monitored and supervised.
- You must return the laptop to school for regular health checks or when requested and ensure that the laptop antivirus software is updated by the school ICT technician's (automatic updates to be reviewed by the Agilisys at least annually).
- At the request of the School or Agilisys you must ensure your laptop is accessible to perform maintenance or updates.

- Passwords should be kept safe. Update your passwords regularly and don't let others use them.
- Return the laptop before leaving the employment of the school.
- Report any possible security breaches (eg. laptop stolen or misplaced) to the Head Teacher or Executive Manager immediately.
- Ensure that the school office has noted any serial numbers for the equipment and asset tags have been created, where necessary.
- Back up your files regularly and store them securely through the means of the Google Drive to ensure you do not lose your data in the event of loss, damage or theft.
- Do not allow family or friends to use your laptop, as there is a risk that school information could be compromised.
- **If you are attacked, don't risk your own safety. Hand over the laptop or device. It can be replaced but you can't.**

School Responsibility

It is the responsibility of the School and Agilisys to ensure the correct configuration of school-owned laptop devices. The teacher is responsible for ensuring the integrity of the configuration that had been set up by Agilisys (e.g. not installing unauthorised software). The school will be responsible for:

- Operating a "health check" programme where laptops are recalled at least annually. The configuration of the laptop will be checked, and any necessary software upgrades completed. The teacher must cooperate with the school and ensure that both school-owned devices (which can carry viruses into the school system etc) are made available for checking.
- The school will keep a list of serial numbers for laptop devices and will notify the police if a school-owned device is stolen. The school will obtain a crime reference number and advise the school's insurers.
- The school will keep a list of help desk numbers/contact information (e.g. telephone numbers or website addresses to report thefts, cancel service and report faults).
- Ensure that the school's approved Anti-Virus software is installed (where appropriate) at the time of issue to staff. The anti-virus system must be updated on an annual basis. It is the responsibility of the teacher to monitor this, and to contact the school ICT co-ordinator if they believe this is not occurring. In no circumstances shall the user delete or disable the anti-virus software.
- Providing encrypted USBs or encrypted storage for staff members.

Use of the internet

The school's "Internet Usage Policy" applies to school-owned computers, whether used on the school network, at home, or in any other location. Please refer to this policy for more details.

If you are deemed to be responsible for a breach in the agreement that contributes to the loss, damage or theft of a device you could be liable for the replacement cost. In signing this document you agree to the particulars of the agreement as part of your employment with The Westminster School.

Signed _____ Date _____

Print Name _____

Glossary

Authorised User:

A user who has been authorised to use the laptop, by being either the designated owner of the laptop, or a member of staff who has been given permission by the designated owner to use the laptop.

Unauthorised software:

This is software that has not been authorised for use or installation by the Head Teacher, ICT co-ordinator or ICT Technician.

Unlicensed software:

This is software for which the school or user does not possess a license (including downloads from the internet – please see the Internet Usage Policy for more details), and therefore has no legal entitlement to use. The use of such software would leave both the school and the individual open to legal action which could result in a heavy fine, or even imprisonment.