Policy Title	Acceptable Use of ICT
Contact person & role	Director ICT
Approval body / Approver	SMG/SLT
Date approved	22 May 2018
Next review by	May 2021

PURPOSE

Westminster School ("the School") aspires to be the best school for an exceptional, all-round education. Achieving this requires the provision of laptops to staff for use:

- to carry out their required duties and functions
- in the preparation for and delivery of curriculum
- to record and track student performance
- to communicate on professional issues
- for appropriate personal, private use

This policy is designed to ensure the proper use of Westminster laptops and ensure the minimization of technological risks to the school, such as breach of privacy, theft of information, impact of viruses, etc.

SCOPE

This policy applies to all staff provided with a Westminster laptop.

POLICY

General

Each laptop will be configured:

- to enable access to the network (both fixed and wireless)
- with School approved anti-virus software
- with all approved software necessary for your role
- to receive regular preventative maintenance when connected to the School network

Staff will have sufficient administrative access to the laptop to allow the installation of additional software for their use. The objective is to allow the laptop to become the staff member's primary work-related computer, with flexibility for reasonable personal use.

Reasonable personal use is permitted where that use:

- Does not interfere with the duties of the employee or his/her colleagues
- Does not interfere with the operation of the school
- Does not compromise the security of the school systems
- Does not impact on the school's electronic storage capacity
- Does not decrease the school's network performance
- Corresponds to all of the school's policies and procedures
- Conforms to the school's practices for file management and storage
- Does not incur any additional expense for the school
- Does not violate any laws
- Does not compromise any confidentiality requirements of the school

By installing additional software, the staff member is confirming that they are appropriately licensed to use that software. The ICT team do not provide support for non-standard software installed by staff.

If a staff member wishes to have additional software necessary for the performance of their duties installed, application should be made through the appropriate process on Inspire i.e. personally acquired and installed software shall not be used for teaching purposes except in a short term 'proof of concept' situation.

All physical maintenance of the laptops shall be the responsibility of and carried out by the School ICT staff.

Any problem with the operation of the laptop should be reported to ICT via the online helpdesk system. ICT staff shall endeavour to fix the problem 'in situ' but shall resort to re-imaging the laptop if no immediate resolution is available. This will result in the need for staff to re-install any private software.

All staff members must accept full responsibility for their allocated laptop whilst in their care. The School's insurance will cover the laptop whilst away from School (other than in the open air) and it is a requirement that the staff member assist the insurer by providing information to assist with the processing of a claim. This assistance may include the details of a police report associated with the loss.

Staff must ensure that laptops are stored in a secure place at all times if left on the campus overnight or for an extended period.

When staff take the laptops away from school, they should ensure the laptop is stored securely when not in use, not left unattended in public areas or left in vehicles.

Staff taking extended leave (10 consecutive weeks or greater) must return the allocated laptop for use by the school in their absence.

If travelling interstate or overseas while on leave, staff must seek SLT approval to take their laptop with them, due to the increased risk of damage or theft. Travelling on planes and in cars can add to the risk of the laptop being damaged, stolen, hacked or infected.

If travelling for work, please confirm the location you are going with the ICT team in order to evaluate the ICT risk of that location and the appropriate measures to be taken to minimise risk.

Upon leaving the employ of the School, staff members must return the allocated laptop, and associated accessories, to the ICT team prior to their last working day at the School.

Ethical and Legal Use

All network and internet use, including email, shall comply with School policies and state and federal laws, including those relating to child protection, privacy, duty of care, anti-discrimination, anti-racism, copyright and harassment. It is particularly important that all software use shall comply with the School's licensing agreements.

Storage or communication of inappropriate material, including pornography, threatening, sexually explicit or harassing materials, offensive or discriminatory materials, or material that may be harmful either physically or emotionally including bullying or harassment of work colleagues is not permitted.

Unauthorised advertising or promotion of personal products or services is not permitted. The laptop shall not be used for non-School commercial purposes without the consent of the Principal.

It is the responsibility of each staff member to report to a School Leadership Team member and ICT any evidence of a breach or potential breach of security and/or misuse of School information or equipment.

Any form of electronic communication has the same legal standing as print copies. The employer has the legal right to examine any such communication created, received or transmitted on school equipment.

Employees are required to limit and periodically review the amount of data they have stored electronically.

Privacy and Confidentiality

Staff members may assume that, in the normal course of events, files in their home directory are confidential. People with access to files (Principal, Director ICT, system administrator and others) will not normally access them without due cause.

Westminster conducts surveillance of the ICT facilities (other than the content of telephone calls). As part of this, all actions performed using the ICT facilities (except for the content of telephone calls) can be logged and may be monitored by the School, or by another person on the School's behalf, on an ongoing basis. You should expect this surveillance to be continuous and ongoing. This includes document creation and deletion, file management, email and other electronic communications which are sent or received, both internally and externally, and internet activity (including the sites visited, the content of those sites and the time spent at each site). The School considers that such surveillance is appropriate to allow it to, among other things, enforce its policies to prevent the use of proprietary software or copies of electronic texts or images in disregard of copyright restrictions or contractual obligations; to safeguard the integrity of computers, networks and data either at the School or elsewhere and to protect the School against any untoward consequences.

EXCEPTIONS TO THE POLICY

Exceptions to this Policy must be approved in advance by the Senior Leadership Team.

CONSEQUENCES FOR POLICY BREACHES

This is a binding document. Failure to comply with this policy may lead to action under Westminster School's Discipline Policy. Breaches of this policy may result in formal disciplinary action being taken.