INSPIRATIONAL
Box Hill School

ICT ACCEPTABLE USAGE POLICY

Last updated: September 2024

Date of next review: September 2025

Authors: Stuart Ansell – Chief Operating Officer and Clerk to the Governors &

Trush Patel – Head of I.T. Services

Box Hill School
IT ACCEPTABLE USE POLICY

This policy and procedures document relates to the network, all connected equipment, any telephones or tablets and any other equipment owned and managed by the IT Services Department.

Computers

- All computers connected to the network are subject to this policy and procedures document. School owned laptops, school managed 1 to 1 scheme devices, iPads, and BYOD (bring your own device) used in school shall be subject to parts of this document, notably the sections on virus policy, email and internet access.

- No cables, peripherals or other hardware should be removed from or added to the school computers without prior instruction by the IT Services Department.

- No software should be installed on school managed computers without prior consultation with the IT Services Department. Any unauthorised software will be removed.

- You must give up use of any school owned and managed device required by the IT Support Staff for the purposes of maintenance.

Software

- Relevant software is provided by the IT Services Department. The addition of other software to the school desktop computers, laptops, iPads and/or the network is only allowed following consultation with the IT Services Department and with the prior approval of the Head of IT Services.

- Users are responsible for the purchase of any licenses that may be required by software on their own machines. The school will not install or provide any software that is

- Student BYOD (Bring Your Own Device) - Only authorised devices can be used within the school and connected to the school Wi-Fi network. All personal devices will be subject to monitoring for safeguarding and cyber security risks.

Other Equipment

- You must only use the equipment owned or managed by the IT Services Department for the purpose for which it was designed. You may be liable for any damage you cause to any item of equipment.

- Personal computers and mobile devices are not supported by the IT Services Department.

- Personal mobile broadband 4G/5G routers are not allowed to be setup and used to bypass the school security systems.

Viruses

- All devices connected to the network must have valid and current anti-virus software installed. Laptops that do not conform are not permitted to connect to the school network.

Any user who knowingly installs or transmits a virus through the school network will be deemed to be in breach of this policy and subject to disciplinary procedures. Network Accounts and E-mail

- Every pupil and staff member is provided with a network account, giving access to various IT resources including a School e-mail account. The use of e-mail as a communication tool is actively encouraged. Any problems resulting in the non-operation of your account should be reported to the IT Services Department as soon as possible.

- It must be pointed out that the provision of a network account is a benefit that may be withdrawn as a sanction if appropriate, resulting from disciplinary procedures. The reinstatement of accounts will be at the discretion of the Headmistress.

- Other 'system' accounts, such as the administrator's accounts and any test accounts or 'suspended' accounts, are only to be used by the IT Services Department. Accounts provided for suspended users to have access during lessons must only be used during those lessons.

- Students whose accounts have been suspended must not use the School network under any circumstances, unless given express permission by the Headmistress. It is not acceptable to use somebody else's account.

- You must only use the account set up for you. Any account that is suspected of being used by more than one user will be suspended. You should not reveal your password to anyone and must not allow others access to your account.

- Your account may be suspended, either temporarily or permanently, for a variety of reasons. If you are unable to access your account, you should inform the IT Services Department.

- Accounts will be monitored, both for usage habits (hours of use and length of time), and content.

Internet Access

 The School provides Internet access for research and educational use. The content of sites visited is monitored and filtered. Common sense is urged when using the Internet, but misuse may result in its availability being withdrawn.

Use of E-mail

- E-mails should not be regarded as private, and any e-mail sent through the school network remains the property of the school.

- All emails are electronically scanned for content, by both an anti-virus program and a content filter.

- You must not use your school email address for personal use.

Network Security

- The school provides its services on trust. If this trust is abused, the network security will be tightened.

- You must not reveal your network password to anyone, or in any way allow your network username and password to be used by anyone. You will be responsible for any actions taken using your username and be subject to any subsequent sanction.

- All user accounts are regarded as private and any material within them are the property of the school. They may be inspected or altered in the course of routine maintenance or for any reason in the course of the school's business from time to time.

- Anyone caught or suspected of 'hacking' or attempting to 'hack' the network in any way will be dealt with according to the relevant disciplinary processes of the school. The definition of 'hacking' for the purpose of this document is "any unauthorised access to any file or resource, whether damage is caused or not". This can include using someone else's laptop without permission, using someone else's network username (even with their permission), or accessing any file deemed to be "out of bounds". The definition of such files is at the school's discretion, so common sense should be applied.

CODE OF PRACTICE

You must not reveal your password to anyone else or allow them to use your network account under any circumstances. You will be held responsible for any action taken using your account.

You must set/change your network password to one that you can remember.

The school network, and all of the data contained within it is the property of Box Hill School. This includes your personal work areas and email mailboxes. These may be checked and altered at any time to preserve the integrity and smooth running of the network. Your permission will not be sought in these instances.

You must take care when using any piece of school equipment. You will be charged for any damage you cause. This damage will include a labour charge, at a rate determined by the Chief Operating Officer.

You must not eat or drink near any piece of computer equipment, including printers.

You must not unplug any cable (electric or data) without prior permission from a member of staff. You must plug the cable back in when you have finished.

You must not turn off any piece of equipment without instruction from a member of staff.

You must not access, delete, move or amend any file that does not belong to you, without instruction from a member of staff.

Internet access is provided to all staff and students. You must use common sense when using this resource. The school maintains a filtering policy, and some sites may be filtered for the protection of all pupils. All Internet activity within the school is logged, and these logs are reviewed on a regular basis.

I.T Services Department
Reviewed: September 2024

Next Review: September 2025