ACCEPTABLE USE POLICY

BROMPTON ACADEMY

VERSION 2

WRITTEN BY DAVID MILLS

INTRODUCTION

This Acceptable Use Policy (AUP) for ICT systems is designed to protect Brompton Academy (BA), our employees, students and other partners from harm caused by the misuse of our ICT systems and our data. Misuse includes both deliberate and inadvertent actions.

The repercussions of misuse of our systems can be severe. Potential damage includes, but is not

limited to, malware infection (e.g. computer viruses), legal penalties and lost productivity resulting from network downtime.

Everyone who works at Brompton Academy is responsible for the security of our ICT systems and the data stored on them. As such, all employees must ensure they adhere to the guidelines in this policy at all times. Should any employee be unclear on the policy or how it impacts their role they should speak to the Director of Learning Technology or the Systems Manager. Every employee should read this in conjunction with their contract of employment regarding the use / misuse of ICT technologies and interactions with students.

2

SCOPE

This is a universal policy that applies to all users and all systems. For some users and/or some systems a more specific policy exists: in such cases the more specific policy has precedence in areas where they conflict but otherwise both policies apply on all other points.

ICT Services who monitor and enforce compliance with this policy are responsible for ensuring that they remain compliant with relevant national legislation at all times. BA reserves the right to change, amend and add to this policy to ensure it stays fit for purpose. BA will inform all users of changes to this policy.

Users who wish to opt out of this policy must discontinue use of all devices covered by this policy and inform the Director of Learning Technologies. If the user is also a custodian then they must also return all hardware that has been issued.

3

USE OF IT SYSTEMS

All data created or stored on BA systems is the property of BA. Users should be aware that BA can't guarantee the confidentiality of information stored on any Brompton Academy system except where required to do so by law.

The BA systems exist primarily to support and enable the education of our students and the efficient management of our Academy. Personal usage and access is limited as per the terms and conditions written in the BA employment contract.

If employees are uncertain about anything regarding any of the ICT systems they should consult ICT Services.

Any information that is particularly sensitive or vulnerable must be encrypted and/or securely stored so that unauthorised access is prevented. However this must be done in a way that does not prevent (or risk preventing) legitimate access by all properly authorised parties.

ICT Services can loan appropriate encrypted USB storage devices to facilitate this.

BA can monitor the use of its ICT systems and the data on it at any time. This may include but is not limited to examination of the content stored within the email and data files of any user and examination of the access history of any users.

Brompton Academy reserves the right to regularly audit networks and systems to ensure compliance with this policy.

4

DATA SECURITY

If data on the BA systems is classified as confidential, this should be clearly indicated within the data and/or the user interface of the system which is used to access it. Users must take all necessary steps to prevent unauthorised access to confidential information (e.g password encrypted emails).

ICT Services will provide information on email encryption upon request.

Users are expected to exercise reasonable personal judgement when deciding which information is confidential. This applies to personal devices which are enabled with access to BA systems and therefore data - Sims, emails (e.g. designated ‘strong’ passwords must be set on personal phones). If in any doubt however, contact the Principal / Vice Principal / Director of Learning Technologies.

Users must not send, upload, download, remove on portable media or otherwise transfer to a non BA system any information that is designated as confidential or that they would reasonably regard as

being confidential to BA, except where explicitly authorised to do so in the performance of their regular duties.

Users must keep passwords secure and not allow others to access their accounts. Users must ensure all passwords comply with the ‘Password/Pin Codes’ part of this document.

Users who are supplied with computer equipment by BA are responsible for the safety and care of that equipment and the security of software and data stored on it and on other BA systems that they can access remotely.

Information on portable devices, such as laptops, MacBooks, tablets and smartphones, is especially vulnerable. Special care should therefore be exercised with these devices: sensitive information stored should be encrypted. Users will be held responsible for the consequences of theft or disclosure of information on portable systems entrusted to their care if they have not taken reasonable precautions to secure it (e.g password must be applied to all personal devices which have BA email / data enabled).

All workstations (desktops and laptops) should be secured with a lock-on-idle policy active after at most five (5) minutes of inactivity. In addition, the screen and keyboard should be manually locked / logged out by the responsible user whenever leaving the machine unattended.

Users should take all actions necessary to ensure that they are at all times properly protected against known threats and vulnerabilities as far as is reasonably practicable and compatible with the designated purpose of those systems (e.g Using P2P software and having virus protection software on home computers if data / files are being transferred using USB keys or other similar method).

Users must at all times guard against the risk of malware (e.g. viruses, spyware, trojan horses, rootkits, worms, backdoors) being imported into BA systems by whatever means and must report any actual or suspected malware infection to ICT Services immediately (e.g bringing in / opening corrupted files / viruses).

5

UNACCEPTABLE USE

The activities below are provided as examples of unacceptable use, however it is not exhaustive. Should an employee need to contravene these guidelines in order to perform their role, they should consult with and obtain approval from a member of SLT before proceeding.

- All illegal activities; these include theft, computer hacking, malware distribution, contravening copyrights and patents and using illegal or unlicensed software or services. These also include activities that contravene data protection regulations.
- All activities detrimental to the success of BA; these include sharing sensitive information as well as defamation of BA.

- All activities for personal benefit that have a negative impact; these include activities that slow down the computer network (e.g. unauthorised streaming video, playing video games, downloading photographs / films).
- All activities that are inappropriate for BA to be associated with and/or are detrimental to BA's reputation. These include pornography, gambling, inciting hate, bullying and harassment.
- Circumventing the ICT security systems and protocols which BA has put in place.
- Accessing of social media such as Facebook, Twitter or LinkedIn unless required to do so in the line of duties. A list of approved staff can be found in Appendices 1 & 2.
- Only authorised staff are permitted to move BA hardware (e.g. ICT Services).

Lack of care / respect for BA equipment (e.g. where provided, always using BA protective cases, otherwise covering equipment with appropriate cases to extend product life).

Applying good 'keep safe' rules to equipment used at home and in the Academy - for instance never leaving iPads / Mac Book on chairs / sofas; always placing them on a hard surface / table. Always using them away from the dangers of liquid damage.

6

MOBILE DEVICES

Mobile devices, such as smartphones, tablet computers (iPads) and Laptops (MacBook Pros / Air) are important tools for BA, however mobile devices also represent a significant risk to information and data security. If the appropriate security applications and procedures are not adhered too they can be a conduit for unauthorised access to BA data and ICT infrastructure. This can subsequently lead to data leakage and system infection.

BA has a requirement to protect its information in order to safeguard its users and reputation. This section outlines a set of practices and requirements for the safe use of mobile devices.

This includes all mobile devices, whether owned by BA or not, that have access to the Academy network, data and systems (e.g. personal phones).

BA reserves the right to install any maintenance or management software on devices that have access to any part of the Academy Network. BA also reserve the right to monitor, track, locate and interrogate any of these devices at any time in any location.

It is the custodian's responsibility to protect any BA hardware assigned to them, this includes, but is not limited to iMacs, MacBooks, chargers, peripherals (such as mice and keyboards) and remote controls.

Under no circumstances is any BA hardware to be left unattended.

No BA hardware is to be left in a motor vehicle.

Custodian should take extra care when using BA hardware on any form of public transport.

All damages, no matter how small, must be reported to ICT services within twenty-four hours of discovery via a damage reporting form.

Custodians are responsible for the care of the device as detailed within this document.

Custodians are not permitted to stick or glue anything to equipment under their care.

It is the responsibility of the custodian to replace any damaged, missing, stolen hardware in the event any of the above conditions have been breached. All replacements must be genuine like-for-like purchased at an officially recognised retailer. All iPad replacements must be MFI certified. If in doubt please seek advice from ICT Services.

Devices must use the most up to date operating systems under the instruction of ICT Services.

Devices must have a strong password that complies with BA's password policy.

Users must ensure that 8GB or ½ (whichever is greater) of BA issued 'device memory' is reserved for work related apps and documents. They must also ensure that 1GB of free memory is available at all times - to facilitate installation of apps.

Users must report all lost or stolen devices to ICT Services immediately.

If a user suspects that unauthorised access to Academy data has taken place via a mobile device this must be reported to ICT Services immediately.

Devices must not be jailbroken or have any software/firmware installed which is designed to gain access to functionality not intended to be exposed to the user.

Users must not load pirated software or illegal content onto their devices.

Applications must only be installed from official platform-owner approved sources (eg. AppStore for iPad and MacStore for MacBooks), Installation of code from un-trusted sources is forbidden. If you are unsure if an application is from an approved source contact ICT Services.

Devices/Apps must be kept up-to-date with manufacturer or developer patches/updates. As a minimum users should check for and apply updates at least once a month.

Devices must not be connected to a PC which does not have up-to-date and enabled anti- malware protection (i.e. Anti-virus software must be installed).

Users must be cautious about the merging of personal and work email accounts on their devices. They must take particular care to ensure that BA data is only sent through the BA email system. If a user suspects that BA data has been sent from a personal email account, either in body text or as an attachment, they must notify ICT Services immediately. (You must have a passcode enabled on your personal devices if they have had BA email enabled / carry BA data.)

Users must not use BA workstations to backup or synchronise device content such as media files unless such content is required for legitimate business purposes.

All staff issued with a BA mobile device must enable any and all mechanisms to protect their device. For iPads 'iCloud Backup', 'Find my iPad' and 'Activation Lock' (post iOS 7) must be enabled.

All users are responsible for protecting their data on mobile devices. This includes but, is not limited to backing up iOS devices overnight and reporting to ICT Services in the event a backup fails.

Users are also expected to replace any damaged peripheral such as chargers assigned to them in the event the original is lost, stolen or damaged. All replacements must be MFI certified (iPads). If in doubt please seek advice from ICT Services.

APPLEID

It is a requirement that every iPad user at BA has an AppleID. To that end every user is expected to sign up for an AppleID using their BA Email Address. Once this is done it must be disclosed to ICT Services, this is so necessary software can be made available as required. The AppleID will be recorded on any system deemed necessary and will be assigned to the user and iPad on these systems.

8

PASSWORD / PASSCODES

Passwords are an important aspect of computer security. A poorly chosen password may result in unauthorised access and/or exploitation of BA's resources. All system users, including volunteers, contractors and vendors with access to BA's systems, are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

The purpose of this section is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change.

- Key system-level passwords (e.g. root, Windows Administrator, application administration accounts, etc - these are largely specific to ICT Services) must be changed on at least a yearly basis where possible.

- All user-level passwords (e.g. email, web, desktop computer, etc.) should be changed every six months and at least on a yearly basis.
- User accounts that have system-level privileges granted through group memberships or programs must have a unique password from all other accounts held by that user.
- All user-level and system-level passwords must conform to the official guidelines.

Guidelines

All users at BA should use strong passwords.

A strong password should contain at least five characters of which three are from the five following classes;

- Lower case characters
- Upper case characters
- Numbers
- Punctuation
- Special characters (@#$%^&*()_+|~-=\`{}[]:";<>/)

Weak passwords are not to be used. A weak password would be a word found in a dictionary or any of the following;

- Names of family, pets, friends, co-workers, fantasy characters, etc.
- The words "Brompton", "Academy", "Teacher", "Student" or any derivation.
- Birthdays and other personal information such as addresses and phone numbers.
- Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
- Any of the above backwards.
- Any of the above preceded or followed by a digit (e.g. Teacher1, 1Teacher)

One way to create a good password is to base it on a song title, affirmation, or other phrase. For example, the phrase might be "Schools Out For The Summer" and the password could be: "SO4tS!" or some other variation.

(Please don’t use the above example as a password!)

All passwords are to be treated as sensitive, confidential BA information.

Passwords should never be written down or stored on-line without encryption.

Do not reveal a password in email, chat, or other electronic communication.

Do not speak about a password in front of others.

Do not hint at the format of a password (e.g. "my family name")

Do not reveal a password on questionnaires or security forms.

If someone demands a password, refer them to this document and direct them to the ICT Services.

Always decline the use of the "Remember Password" feature of applications.

If an account or password compromise is suspected, report the incident to ICT Services

The only exception to this policy is if a service supports a different password requirement (seek explicit advice from ICT Services regarding this).

How to Change your Password

Changing your password can be done at any time my visiting the fingerprint scanner near the iBar. Simply scan your finger and select ‘Reset Password’ when prompted. Your current password will then be reset to ‘Password123’.

Then the very next time you log on to an iMac you will automatically be asked to select a new Password.

EXTREMISM

All users have a responsibility to protect our young people from extremism. ICT Services blocks access to such material as soon as it is identified by the Office of Security and Counter-Terrorism branch of the UK Home Office. If any user becomes aware of such material being accessed via any method, it must be reported to Refer Now or Emma Perkin .

10

ENFORCEMENT

Any employee found to have violated this policy may be investigated under the Academy discipline policy, this may lead to misconduct / gross misconduct charges which could lead to written warnings or dismissal. Failure to correct the violation will result in access to the BA system being limited or disabled and confiscation of any BA issued devices.

BA will not tolerate any misuse of its systems and will discipline anyone found to have contravened the policy, including not exercising reasonable judgment regarding acceptable use. Employees should be aware that under the formal disciplinary procedures consequences may include termination of their employment.