Technology Acceptable Use Policy - Stephen Perse 6th Form College

This policy applies to all students attending the Stephen Perse Foundation (the **Foundation**) 6th Form College (the **College**).

Glossary

BYOD	Bring your own device

Introduction

Technology is provided for students to complete homework, support their learning, conduct research and communicate with others for educational purposes. Students are responsible for anything they do when using technology just as they are in a classroom or corridor. They should always comply with the Foundation's standards and remember that access is a privilege, not a right and that access requires responsibility for their behaviour.

This policy refers to all technology including iPads, PCs, Google Apps and mobile phones.

To help ensure full understanding from students, the sign off sheet (at the end of this Policy) requires signing annually by all new and existing students at induction.

Guiding Principles

Technology can be a valuable educational tool, conferring many benefits which enhance teaching and learning. It provides opportunities for students to conduct research and communicate with others for educational purposes.

Use of Technology (including Foundation provided iPads or BYOD)

Appropriate sanctions, as outlined in our Behaviour and Discipline Policy, will be imposed for any misuse of technology. Examples of misuse would include:

- disseminating material without permission
- taking photographs without permission
- making recordings without permission
- any activity in furtherance of cyber--bullying
- gaining access to inappropriate internet sites
- any activity that could compromise the Foundation and/or its systems
- any irrelevant/non-educational activity during lessons, such as playing games
- communicating electronically in lessons with other students without permission

This list is illustrative rather than exhaustive.

Technology may be used in lessons with the permission of the member of staff and in accordance with

his/her instructions. Digital work should be stored in a Foundation Google Drive account as part of the Google Apps for Education domain.

General Guidance

1. Students must not engage in any use of IT related to cyberbullying (an aggressive, intentional act carried out by a group or individual using electronic forms of contact repeatedly over time against a victim who cannot easily defend him/herself) e.g. unwanted emails. In serious cases of cyberbullying a student may be suspended or excluded.
2. Do not enter into any newsgroups, 'chat' or interactive messaging discussion areas or file sharing services without permission from a member of staff.
3. You will have access to a wide variety of apps and software on your school devices, some of which require signing in. Never give out personal information about yourself or others without first discussing with a parent or guardian. If you are asked to input an address or contact number please use the following - *Address: The Stephen Perse Foundation, Union Road, Cambridge CB2 1HF - Telephone: 01223 454700.*
4. Always tell a member of staff at once if you encounter inappropriate or offensive material.
5. Use of the Internet to create, distribute, store or access inappropriate matter, such as pornographic, racist or offensive material is strictly forbidden. Never attempt to advertise, buy or sell goods, gamble or advertise using the internet.
6. Accessing the internet via home Wi-Fi is permitted. Access to the internet in College should only be made via the 'SPF' authorised Wi-Fi and your password should not be disclosed to anyone or any attempt made to access another user's account.
7. Ensure all portable devices are stored securely on and off the Foundation premises.
8. Activity which threatens the integrity of the Foundation's IT systems, or activity which attacks or corrupts other systems, is strictly forbidden e.g. installation of software / downloading inappropriate files.
9. Foundation e-mail can only be used for legitimate College-based purposes and personal e-mail addresses may not be used in College lesson time.
10. Do not respond to unpleasant emails.
11. To guard against viruses when using e-mail, always delete without opening mail from anyone unknown to you. Also delete any 'chain letters' you may receive - never forward them on to your friends.
12. Copyright of materials and intellectual property rights must be respected. If unsure, students must seek advice from staff.
13. iCloud backup must be switched on for iPads. In addition please ensure all work is backed up to your College Google Drive.
14. Internet filtering is managed in line with government guidance.
15. Further support and guidance can be found here: http://www.saferinternet.org.uk/advice-and-resources/young-people
16. Passwords should be complex, please refer to the password policy in this document.

17. You must protect all of your Foundation related computer accounts. Do not leave yourself logged in unattended on any device (at home or at College). A strong password (see above) or biometrics must always be used to protect access to your accounts. They should never be accessible directly without this, especially if you have saved a password or access code to a browser or app.
18. Two Factor Authentication must be enabled on your Google account. It must also be enabled on all SPF accounts that access sensitive or personal data where available.
19. Any device provided by the Foundation is the property of the Foundation and is to be returned when an individual leaves the Foundation.
20. If you have lost a device with access to Foundation accounts on report it to the Foundation immediately.

Student's Personal Electronic Devices

The Foundation cannot take responsibility for the loss or damage to personal electronic devices, including mobile phones. Emergency messages from parents or guardians to students should be given to the College Office and no student can therefore state a need to have a mobile phone switched on whilst in the College.

Parents and students should be aware of potential risks such as theft, bullying and inappropriate contact, including grooming by unsuitable persons. Parents and students are therefore encouraged to ensure that suitable filtering devices are activated on mobile phones and similar devices. If a personal mobile device contains access to Foundation data it must be protected by a password or fingerprint.

It is recognised that there are many benefits from having access to mobile technology and that items such as mobile phones have become regarded as a necessity in certain circumstances e.g. for students with long or awkward journeys. The Foundation requests mobile phone contact details from each student as part of our emergency communications plan such as may be used in the event of sudden closure of the College during inclement weather. Mobile phones should be silenced and should not be used during lessons, tutorials, assemblies or any like gathering unless with the teacher's permission. Mobile technology must not cause disruption to others when they are used in the public places in the College e.g. Coffee Shop or Library.

If a mobile phone rings or receives a communication during a lesson or activity a warning will be given. In the case of a student continuing to ignore such warnings, the phone will be confiscated for the remainder of that College day. Staff should bring confiscated phones to the College Office.

Students are requested not to use their mobile devices for capturing images or videos. If they are used, the permission of any and all those, students or staff, included in the images must be expressly sought. Mobile phones and other devices should never be used for the filming of illegal activity or for the downloading, storing or forwarding of indecent images or the accessing of inappropriate websites. Posting or dissemination without material without permission will be counted as misuse.

Searching, screening and confiscation

Students' electronic devices may be searched in accordance with the Behaviour and Discipline Policy. Where the person conducting the search finds an electronic device that is prohibited by the College Rules or that they reasonably suspect has been, or is likely to be, used to commit an offence or cause personal injury or damage to property, they may examine any data or files on the device where there is a good reason to do so. They may also delete data or files if they think there is a good reason to do so, unless they are going to give the device to the police.

In determining a 'good reason' to examine or erase the data or files the staff member should reasonably suspect that the data or file on the device in question has been, or could be, used to cause harm, to disrupt teaching or break the College Rules.

If an electronic device that is prohibited by the College Rules has been seized and the member of staff has reasonable grounds to suspect that it contains evidence in relation to an offence, they must give the device to the police as soon as it is reasonably practicable. Material on the device that is suspected to be evidence relevant to an offence, or that is a pornographic image of a child or an extreme pornographic image, should not be deleted prior to giving the device to the police.

If a staff member does not find any material that they suspect is evidence in relation to an offence, and decides not to give the device to the police, they can decide whether it is appropriate to delete any files or data from the device or to retain the device as evidence of a breach of Foundation discipline.

Parents are informed when such a search has taken place and a record is kept of the incident, including the reasons for the search and its outcome.

The College does not tolerate any form of bullying including cyberbullying and the welfare of the students is of paramount concern.

Access to the web outside of the Foundation may be directed through the Foundation's web filtering system. Access through the Foundation's filtering system results in the collection of web history and IP address information.

Access Cards

Students are issued with an Access Card for door entry and printing which for security purposes must be reported immediately if lost or stolen. The first loss in an academic year is not charged but the charge for a second loss is £5. The charge for a third loss in an academic year or any beyond that is £10 for each loss. Charges will be collected through our Finance Department.

stephen perse
foundation

Foundation iPads

The Foundation leases the iPads provided for students and they must be returned in good working order with no damage. Students are responsible for the safety of their iPad. It must be securely locked away and hidden when unattended. A protective case is provided and the iPad must be kept in it at all times. Students are not allowed to decorate the case or iPad. If a student's iPad is lost or damaged it must be reported to the IT Department at the Senior School as soon as possible. Loss or damage charges apply in line with our leasing company's guidelines for return and are as follows:

Grade A - £10: Replacement for charger plug or cable.
Grade B - £75: Screen damage (cracks, shattered glass etc).
Grade C - £150: Damage to the iPad that is beyond a screen replacement. Examples include a bent device, damage to internal components, damage that would void the iPad warranty etc.
Grade D – Full cost of replacement: Loss of device, negligence leading to loss of the device, deliberate damage to the device or failure to return the device when requested.

In the event of the iPad being forcibly taken by attack, assault or mugging we encourage you to give up the iPad. Please inform the Police and obtain a crime reference number. With a crime reference number we would charge a £50 excess fee, without this number you may be charged the Grade D level. Please let us know as soon as possible so we can put the iPad in lost mode so it can be locked down and tracked.
Charges will be collected through our Finance Department.

Password Policy

This policy applies to any account you have whilst at the Foundation. This could include but is not restricted to, your domain login account, your Google account, any approved third party app etc.

You must:

- Ensure passwords for any Foundation accounts should be at least 8 characters, complex (consisting of 3 of 4 of the following: Uppercase letter, Lowercase letter, Number, Special Character).
- Keep passwords secret.
- Arrange to have your password changed immediately if you suspect someone knows it.
- Log out when away from your system.
- Change account passwords at intervals appropriate to the required security level (we recommend at least termly).
- Ensure any passcodes that are set for devices are not easy to guess (eg. 1234).

You must not:

- Allow others access to IT equipment or Foundation systems logged in with your password.

- Write down passwords in a form that others could identify or in a place it could be stolen from.
- Share passwords.
- Give your password to anyone.
- Allow anyone to watch you typing your password.

Choosing a Password

- Your password must be at least eight characters with a combination of 3 of 4 of the following; upper and lower case letters, a number and special character.
- Do not use a word found in a dictionary, English or foreign.
- Passphrases are recommended, i.e. a sentence that only you would know.
- Never use the same password twice.
- Choose a password that you can remember and type quickly, this reduces the chance of somebody discovering your password by looking over your shoulder.

Things to avoid

- Do not just add a single digit or symbol before or after a word. e.g. "apple1".
- Using the 'Save Password' option in login boxes.
- Do not double up a single word. e.g. "appleapple".
- Do not simply reverse a word. e.g. "elppa".
- Key sequences that can easily be repeated. e.g. "qwerty","asdf" etc.
- Do not just garble letters for easy to guess words, e.g. converting s to $, o or 0. as in "Pa$$w0rd".
- Using the same password for multiple accounts.
- Re-using old passwords.
- Currency signs as this does not sync with some cloud applications like Google.

Poor Passwords

- Do not use passwords based on personal information such as: name, nickname, username, email address, birth date, friends name, hometown, phone number, car registration number, address etc. This includes using just part of your name, or part of your birth date.
- Do not ever be tempted to use common passwords that are easy to remember but offer no security at all. e.g. "password", "letmein".

Please refer to:

Behaviour and Discipline Policy - Foundation
Anti-Bullying Policy - Foundation
Safeguarding and Child Protection Policy - Foundation
Online Safety Policy - Foundation
College Rules

Violations of the above rules may result in a ban on Internet use. Involvement in cyberbullying may result in suspension or exclusion.

Reviewed: November 2018

Version Control

Date of adoption of this policy	5 November 2018
Date of last review of this policy	5 November 2018
Date for next review of this policy	August 2019
Policy owner	IT Manager
Authorised by	Senior Leadership Team

stephen perse
foundation

Technology Acceptable Use Policy (6th Form College)

==========

I have read the Technology Acceptable Use Policy (6th Form College) and agree to abide by it. I understand that any misuse, including involvement in cyberbullying, will be dealt with as described in the Stephen Perse Foundation Anti-Bullying Policy and Behaviour and Discipline Policy.

Student Signature: .....

Student first name: ..... Student last name: .....

Form: ..... School: .....

Date: .....