Stephen Perse

Foundation

Technology Acceptable Use Policy for Students

Contents:

1. The Policy
2. School Specific Rules and Information
   - 2.1. Early Years Foundation Stage (EYFS) and Years 1 and 2
   - 2.2. Years 3 to 6
   - 2.3. Years 7 to 13
   - 2.4. Charges for damage or replacements
3. Pupils' Personal Electronic Devices
   - 3.1. Years 3 to 11
   - 3.2. Years 12 to 13
4. Password Policy
5. Related Policies

1. The policy

This policy applies to all pupils attending Stephen Perse Foundation (the School) including in the EYFS and those who board.

Here at Stephen Perse, we recognise the enormous learning potential provided through the use of technology. We see this as an essential part of the learning and development of our pupils, preparing them for adult life. We realise that whilst there are some incredible tools and learning opportunities online, there are certain rules that must be in place to ensure safe usage. We encourage discovery of a variety of views online in order to form a balanced opinion, but within our overriding ethos of tolerance and respect in line with fundamental British values.

We will always do our best to try and prevent access to inappropriate, offensive and adult material but recognise this is not always possible as no technical solutions are perfect. Therefore the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using technology. We believe it is vital to equip our pupils with the skills and understanding to be smart and stay safe with their decisions and choices online. Pupils are encouraged to report to a member of staff if they come across any inappropriate material, or if they have any safeguarding concerns about themselves or others.

This policy intends to encourage pupils to use IT safely and responsibly and it is illustrative rather than exhaustive. In general, appropriate behaviour doesn't change through the addition of technology; where things go wrong technology is invariably the medium rather than the underlying issue. Pupils should remember that the use of technology is a privilege, not a right, and that its use requires them to take responsibility for their behaviour.

We acknowledge that this policy applies to pupils at very different development stages of their lives, but we will endeavour to cover the broad principles that should apply to all, as appropriate to their age:

- **Relevant and appropriate use -** Use the school IT equipment, network and internet access in relation to your areas of study or interest in line with the values of the school. School email and messaging accounts should only be used for legitimate school related purposes. Contact with staff and pupils should always be through your school accounts and personal accounts may not be used during lessons.
- **Monitoring -** Be aware that any device connected to the School IT network (including personal devices) can be controlled and monitored. Anything you post, access or search online or on the school's IT network and devices (including personal devices) is filtered in line with government advice, and is traceable and may be monitored and/or logged. This information could then be made available on request to members of staff or even the police if your activity is illegal.
- **Legal compliance -** Respect laws, copyright, personal and privacy rights, age restrictions and intellectual property rights.
- **Respect the privacy of others -** in particular not to take, artificially generate or disseminate photos, videos and/or audio recordings of others without the express permission of a member of staff. Impersonating, and posting about others online is a strict violation of this policy.
- **School compliance -** Ensure that your use of technology and online activity both in and out of school does not bring the school into disrepute. You must not post or disseminate anything offensive or defamatory, and your activity must be compliant with the school rules and anti-bullying policy.
- **Suspicious content -** Be careful with links and attachments in email or online, and with QR codes which are used for phishing attacks. If something looks suspicious, do not interact and contact the IT Department for further advice.
- **Circumnavigating security** - Recognise that any attempt at hacking, logging in with

someone else's account, circumnavigation of security or web filtering, tampering, compromising performance or unauthorised access to the school's IT network, its devices or accounts is strictly forbidden. Access to the school's wifi should be via the SPF/SPC/DBs network only, with the exception of 1-11 shared school devices.

- **Personal data protection -** Never give out personal or location information about yourself or others without first discussing it with a parent or guardian. If you are asked to input an address or contact number please use the School details which are as follows: *The Stephen Perse Foundation, Union Road, Cambridge CB2 1HF - Telephone: 01223 454700.*
- **Password protection -** Do not give out your password to friends or log someone in with your account. Protect your accounts and devices with a password only you know that complies with our password policy (*this does not apply to some EYFS and Year 1 to 6 environments, see Password Policy further down*). If you have lost a device with access to school accounts on or your access card, report it to the school immediately. Never leave yourself logged into any device, application or browser unattended or unlocked, and do not save passwords in browsers on shared devices.
- **Backup data** - Ensure that you backup your work to Google Drive. Files stored elsewhere have no recovery facility if lost. You must only ever be logged into your school iPad with a school issued managed AppleID. The school cannot be held responsible for loss of data stored on SPF systems.
- **Protect devices -** Ensure any device issued to you, or personal device on the school's IT network or brought onto a school site has the latest critical security updates installed, and that there is no inappropriate/harmful/illegal content or software on it. Personal devices should have up to date antivirus software, be regularly updated, and on an operating system still supported by the manufacturer.

Use of Artificial Intelligence (AI) technologies

AI technologies offer fantastic opportunities for inspiration, learning and productivity. However, they must be approached with caution, and be used in compliance with the rules below:

- **Critically assess AI produced content** - All generated AI content should be read thoroughly, customised and fact checked where necessary. Content produced by AI should not be considered fact.
- **Cite your sources -** Pupils must ensure that work submitted is demonstrably their own. If any sections of their work are reproduced directly from AI generated responses, those elements must be identified by the pupil.
- **Illegal or Inappropriate Content** - Any use of AI to generate content that breaks laws, school rules, or causes offence, distress or humiliation to others is strictly prohibited. AI must not be used to generate content about others without their express permission.
- **Suspected use of AI -** Producing work inconsistent with previous submissions may raise suspicion and result in pupils being challenged on whether it was produced by AI if not acknowledged. Due to the difficulty in accurately identifying this, there may occasionally be false accusations, however please be aware it is done in the pupils' best interests.
- **Assessments and exams -** Unless stated otherwise, AI must not be used for tests or exams. Its use in NEA or coursework must comply with the latest JCQ regulations https://www.jcq.org.uk/exams-office/malpractice/artificial-intelligence/

Disclaimer: Although pupils may be trusted by their parent(s) or guardian with regard to private internet use, the School has a legal obligation to safeguard the pupils in our care. Professional judgement will be used by the school if it is felt that activity taking place outside of the school's IT network and devices has an impact on the pupil's safety or wellbeing - or that of other pupils or staff - in these incidents we may take disciplinary action or report it to the appropriate authorities. In all disputes the Head of School will be the final arbiter.

2. School Specific Rules and Information

2.1. Early Years Foundation Stage (EYFS) and Years 1 and 2

There are opportunities for pupils to use technology during the school day. Such activities are supervised and monitored. In PSHE, we aim to develop pupils' skills in understanding how to use the internet safely. Staff select and screen sites that the pupils use, independent research is directly supervised.

2.2. Years 3 to 6

Technology should only be used in Years 3-6 with the permission and instruction of a member of staff. Pupils are made aware of the potential dangers of the internet during PSHE lessons and their access to the internet in school is closely supervised, with direction given to recommended websites in lessons and for homework.

Year 6 pupils have a 1:1 provision of iPads in order to prepare them for the Senior School, and have the option to take it home to support their learning, principally through the completion of homework. Any breakages that occur whilst an iPad is not in school will be charged for repair to the parent (see charge details in paragraph 2.4 (iii) in this policy). Parents will need to notify the school that they wish for their child to bring home their school iPad each day, or on specific days. This option will be revoked if the pupil consistently fails to bring the iPad into school for their learning (3 times within a half term period).

Two-factor authentication can be used on your school Google account to add extra security, and on other systems to protect personal data. This could be difficult for pupils of this age, or those who only use shared devices, so we do not enforce it, but it is recommended.

2.3. Years 7 to 13

- All Senior School and Sixth Form pupils are issued an iPad, protective case, screen protector, charging plug, charging lead, access card and lanyard when they join.
- Pupils are responsible for bringing in their iPad each day which should be fully charged. Temporary replacements will not be issued.
- Two-factor authentication must be enabled on pupils' school Google account, and wherever possible in other systems to protect personal data.
- Boarding Houses have enforced curfews for internet access at certain times.

2.4. Charges for damage or replacements (Years 7 to 13)

It is the responsibility of the pupil to keep their iPad, protective case, screen protector, charging plug, charging lead, access card and lanyard safe. For this reason - regardless of fault or where and when the incident took place - the parent(s) or guardian of the pupil are responsible for charges if damaged or lost. We know this can be a cause of concern, but the school heavily subsidises the cost of repairs in a way we believe is fair and consistent. In some cases however, where it is clear another pupil is at direct fault for the damage, we will ask the parent(s) or guardian of that pupil to pay. In all cases, the final decision will sit with the Head of School. Any loss or damage of any school allocated equipment, including access cards, must be reported immediately.

Any damages to iPads must be reported to the IT Department straight away, who will handle any repairs and issue a replacement device once a damage form has been completed. This form is obtained when the damaged iPad is handed in. You should not conduct repairs yourself; only those completed by Apple are valid for our warranty.

(i) Access card

1st loss in an academic year: No charge

2nd loss in an academic year: £10
3rd and subsequent losses in an academic year: £20
Lost lanyard: No charge
KURA Bus Token loss: £5

(ii) iPad accessories

iPad case replacement if graffitied or damaged (i.e. where the cover no longer protects the screen / magnet is not attached): £30 new case + Behaviour Point or £5 refurbed case + Behaviour Point (student/parent choice).
Screen protector: £10
iPad charger if lost or damaged: £10*
iPad charging lead if lost or damaged: £10*
**NB. If you choose to replace the iPad charger and charging lead yourself you must replace them with authentic Apple products. Natural wear and tear is still classed as damage.*

(iii) iPad

Grade A - £80: Screen damage (cracks, shattered glass etc). **A screen protector *must*** be fitted on the device.
Grade B - £200: Damage to the iPad that is beyond a screen replacement, or damage **without a screen protector fitted**. Examples include a bent device, damage to internal components, any damage or actions that would void the iPad warranty etc.
Grade C – full cost of replacement: Loss of device, deliberate damage to the device or failure to return the device when requested.

(iv) Classroom IT Equipment

AV - Damage to school audio/visual equipment: £1000.
PC - Damage to a PC: £500.
MAC - Damage to a MAC: £1000.

Please note:

- In the event of repeated damage to the iPads which indicates a lack of appropriate care is being taken, then repairs would be treated as 'Grade C', and the full costs of replacement or repair would be passed on to parent(s) or guardians.
- In the event of the iPad being forcibly taken by attack, assault or mugging we encourage you to give up the iPad; your safety is much more important. Please inform the Police and obtain a crime reference number. With a crime reference number there would be no fee payable, without this number you may be charged the 'Grade C' rate. Please let us know as soon as possible so we can put the iPad in lost mode in order for it to be locked down and tracked.
- All charges will be collected through our Finance Department and added to fees. Any equipment provided by the school remains at all times the property of the School and is to be returned on or prior to the last day of your enrollment at the school. Any damages when returning the iPad will incur the charges as above.
- iPads should only be charged with the authentic Apple iPad charger provided.
- We will provide a protective folio case and screen protector. If the case is damaged, defaced or worn (either deliberately or through wear and tear) to the point it is unable to protect the iPad screen (the case must be able to fully cover the screen and be closed and locked with the magnet), you must ask IT for a replacement which will be charged.
- Any defacing of the case or iPad is a breach of this policy that will result in sanctions, and you will be charged the full cost of replacement.
- Only the case provided by the School must be used, and ensure the iPad is kept in it at all times and the cover is closed when not in use. If you would prefer a keyboard case, this would have to be purchased yourselves (SEND needs excepted), but first authorised by the Head of Year to ensure the case offers sufficient protection, with only plain cases

accepted.

- All Senior School and Sixth Form student iPads must have a screen protector installed which is fitted by the IT Department, if you do not have one it must be reported straight away or you will be liable to higher fees if the device is damaged. The protector will only be replaced if it is felt the screen is at risk, this assessment will be made by the IT Department. If the screen protector is removed, falls off or is deliberately damaged it will incur a replacement charge.

3. Pupils' Personal Electronic Devices

The School cannot take responsibility for loss or damage to pupils' personal electronic devices. They should not be left visible or unprotected in school, for example on bag racks or in desks.

Parents are encouraged to ensure that suitable filtering systems are activated on mobile technology used by their child(ren). If a personal mobile device contains access to school data, such as school email, it must be protected by a password (compliant with the password policy below) or fingerprint.

Pupils must seek the permission of a member of staff before taking and using their electronic devices to take photographs or make recordings on school premises, or on school activities or trips.

Pupils' electronic devices may be searched in accordance with the School's Behaviour Rewards and Sanctions and Searching and Retention and Disposal of Confiscated Items policies and as set out in the Department for Education document 'Searching, screening and confiscation' (2014, reviewed 2023).

3.1. Years 3 to 11

It is recognised that personal electronic devices (including but not limited to mobile phones, smart watches, tablets, laptops) are necessary in certain circumstances, e.g. for pupils with long or awkward journeys who may need to contact parents en-route. However, they must not be seen during the school day and must be kept in airplane mode or equivalent, and in Y1-6 they must be handed to the school reception at the start of the day. Emergency messages from parents for pupils should be sent to Reception and/or the School Office who will pass these on. In Y7-11, students are permitted to use mobile devices briefly during late stay to make travel arrangements or in exceptional circumstances with permission from a member of staff. Any access to the internet must be via the School's WiFi network - no cellular data usage is allowed.

3.2. Years 12 to 13

The use of personal electronic devices (including but not limited to mobile phones, smart watches, tablets, laptops) in lessons should only be for learning purposes. During this time such devices should be put in airplane mode or equivalent. Whenever on site, students should only connect their devices via the school's WiFi network - no cellular data use is allowed.

4. Password Policy

We recognise that some pupils this policy applies to are very young, would find it difficult to comply with a password policy and don't manage their passwords. Therefore our password policy applies only from Year 3 to Year 13. For years below that, this password policy does not apply but can be used as a good practice guide to set a secure password.

We have set our password policy in line with advice from NIST (National Institute of Standards and Technology), this applies to any school login account you have (e.g. Apple ID, your main computer and Google login). You may find that if you try and set a password that is not NIST compliant it will not let you. The list of compliant passwords changes all the time and will

depend on if they have been involved in a known leak or hack so you may have to try a few different ones. Please follow the guidelines below to find one that works:

- Minimum 12 characters (recommended 16).
- Does not need to be complex (i.e. a combination of upper and lowercase letters/numbers/special characters).
- We recommend using three random words (eg. lexiconcontainerelephant).
- Do not use words that are linked with you or could be guessed (password, qwerty, names, favourite teams or artists etc).
- Do not use currency symbols.
- Do not write passwords down.
- Do not use the same password for multiple accounts.
- It is your responsibility to securely protect your passwords, do not share them or write them down where they can be accessed by others.
- If you suspect someone knows your password, change it immediately.
- Regularly review and remove access for third-party applications or services that no longer require access to accounts.

This policy also applies to iPad passcodes. For pupils who have their own school issued iPad, we recommend that touch ID is set up so those pupils only have to re-enter the password when they restart the iPad.

This policy acts as an extension of the general school rules. Breaches of this policy may result in disciplinary sanctions, in line with the school's behaviour and discipline policy, and in serious cases may lead to suspension or exclusion.

5. Related Policies

- Anti-Bullying Policy
- Behaviour, Rewards and Sanctions Policy
- School/Boarding Rules and Code of Conduct
- Online Safety Policy
- Safeguarding and Child Protection Policy
- Searching and Retention and Disposal of Confiscated Items Policy

Reviewed: January 2025

==========

I have read this policy 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 Rewards and Sanctions Policy. I understand that if I do not follow this policy I may be denied the use of IT facilities or systems for an indefinite period and/or be subject to school sanctions. I understand I may be charged for the cost of putting right any damage I may do to IT equipment or software, whether deliberate or accidental, as a result of not following instructions. This policy is signed at enrollment, and thereafter we will notify you of annual changes but there will be no requirement for a further signature. Access to school systems will not be allowed unless this policy is agreed to.

Student Signature: .....

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

Date: .....

Version Control

Date of adoption of this policy	22 January 2025
Date of review of this policy	January 2025
Date for next review of this policy	August 2026
Policy owner	Chief Information Officer
Authorised by	IT Committee and Heads of Section