Stephen Perse

Cambridge

TECHNOLOGY ACCEPTABLE USE POLICY

Contents:

Stephen Perse

Cambridge

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 value of technology in learning and preparing pupils for the future. While online tools offer great opportunities, rules are necessary 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.

Though we work to block inappropriate, offensive and adult material content, no system is perfect, and the school cannot be held responsible for everything accessed online. Instead, we focus on teaching pupils how to make smart, safe choices. You should report any inappropriate material or safeguarding concerns to staff.

Key Principles

This policy encourages responsible IT use. Technology is a privilege, not a right, and you must act responsibly. The key principles include:

1
Relevant & Appropriate Use

School IT resources must be used for learning purposes. Personal accounts should not be used in lessons; contact with staff and peers should always be through your school accounts and personal accounts may not be used during lessons.

2
Legal Compliance

Respect laws, copyright, personal and privacy rights, age restrictions and intellectual property rights

Monitoring
3

All devices on the school network, including personal ones, can be controlled and monitored. Online activity may be logged and this information could then be made available on request to members of staff or even the police if your activity is illegal.

4
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.

Data Backup
5

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.

6

Respecting the privacy of others

Do not take, share, or post images, videos, or recordings of others without permission. Impersonation and online harassment are strictly prohibited.

7

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.

8

Personal Data

Never share personal or location details without consulting 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.

9

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.

10

Password Security

Keep passwords private and follow the school's policy. If you have lost a device with access to school accounts on or your access card, report it to the school immediately. Always log out of devices, apps, and browsers when unattended, and avoid saving passwords on shared devices

11

Device Security

Ensure both school and/ or personal device that are on the school's IT network have 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

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:

Check AI content carefully

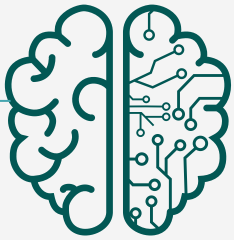
All generated AI content should be read thoroughly, customised and fact checked where necessary. Content produced by AI should not be considered fact.

No harmful or inappropriate AI 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.

Cite your sources

You must ensure that work submitted is demonstrably your own. If any sections of your work are reproduced directly from AI generated responses, those elements must be identified.



AI use may be questioned

If your work is very different from usual, teachers may ask if AI was used. 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.

No AI in exams or tests

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/

Although you may be trusted by your 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 your 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.

Early Years Foundation Stage (EYFS) and Years 1–2

EYFS and Years 1 and 2 Pupils use technology under supervision, with activities carefully monitored. We aim to develop pupils' skills in understanding how to use the internet safely in PSHE. Staff select and screen websites, and independent research is always supervised.

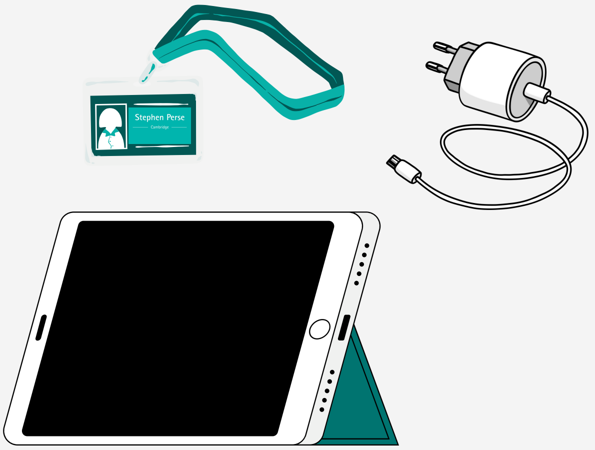
Years 3–6

Technology should only be used in Years 3-6 with the permission and instruction of a member of staff. PSHE lessons cover online safety, and internet access is closely monitored, with pupils directed to appropriate websites for lessons and homework.
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.

Year 6 iPads

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. 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).

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 you join.

You are responsible for bringing in your iPad each day which should be fully charged. Temporary replacements will not be issued. Two-factor authentication must be enabled on your school Google account, and wherever possible in other systems to protect personal data. Boarding Houses have enforced curfews for internet access at certain times.

Charges for Lost or Damaged Equipment (Years 7–13)

Charges for Lost or Damaged Equipment (Years 7–13)

You are responsible for keeping your iPad, accessories, and access card safe. Parents/guardians must cover the cost of replacements or repairs, no matter how or where the damage occurs. However, if another pupil is clearly at fault, their parent/guardian may be charged. The Head of School makes the final decision. All damage or loss must be reported immediately.

Reporting & Repairs

- Report iPad damage to IT immediately. A repair form must be completed before a replacement is issued.
- Do not attempt repairs yourself – only Apple repairs are covered under warranty.

Replacement Charges

(i) Access Cards & Lanyards

- 1st lost card (per academic year): Free
- 2nd lost card: £10
- 3rd+ lost card: £20
- Lost lanyard: Free

(ii) iPad Accessories

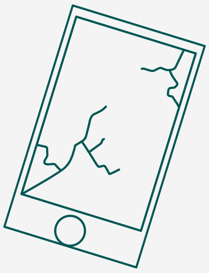
- Case replacement (damaged/graffitied): £30 (new) or £5 (refurbished) + Behaviour Point
- Screen protector: £10
- Charger or charging lead: £10 each (must be replaced with genuine Apple products if buying your own)

(iii) iPad Repairs & Replacements

- (iGrade A (£80): Screen damage (cracks, shattered glass). A screen protector must be fitted.
- Grade B (£200): Severe damage (bent frame, internal damage, or no screen protector fitted).
- Grade C (Full replacement cost): Lost iPad, deliberate damage, or failure to return the device.

(iv) Classroom IT Equipment

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



Important Additional Information

- Repeated damage to iPads indicating neglect will result in repairs being treated as 'Grade C', with full costs passed to parents or guardians.
- If an iPad is taken by attack or mugging, prioritize safety and give it up. Report to the Police, obtain a crime reference number, and inform the school immediately to lock and track the device. Without a crime reference number, 'Grade C' charges may apply.
- Charges will be processed through the Finance Department and added to fees. All school-issued equipment remains the property of the School and must be returned undamaged by the last day of enrollment.
- Only charge iPads with the authentic Apple charger provided. The School provides a protective case and screen protector. Damaged or worn cases that no longer protect the screen must be replaced through IT at a cost. Defacing the case or iPad breaches policy and may result in sanctions and replacement charges. Only the school-provided case should be used unless a keyboard case is authorized by the Head of Year.
- All Senior and Sixth Form students must have a screen protector installed by IT. If missing or damaged, report it immediately to avoid higher fees. Replacements will be made if the screen is at risk, as assessed by IT. Removing or damaging the protector will incur a charge.

Personal Electronic Devices

PERSONAL ELECTRONIC DEVICES

The School is not responsible for lost or damaged personal devices. Keep them secure and out of sight. Do not leave them on bag racks, in desks, or unattended.

↓

Parents should set up parental controls and filtering systems on their child's devices to ensure safe internet use.

↓

The school may search devices in line 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).

↓

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

↓

If a personal device has access to school data (e.g., email), it must be password-protected or secured with fingerprint/Face ID.

Personal Electronic Devices

YEARS 3 TO 11

You might need to bring a phone, smartwatch, tablet, or laptop to school—especially if you have a long journey and need to contact your parents. However, they must remain unseen during the school day, set to airplane mode, and in Y1-6, handed to reception at the start of the day. Emergency messages from parents should go through Reception or the School Office. In Y7-11, mobile devices can be used briefly during late stay for travel arrangements or with staff permission. Internet access must be via the School's WiFi only - no cellular data is allowed.

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, you should only connect your devices via the school's WiFi network - no cellular data use is allowed.

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.

Our password policy follows NIST guidelines and applies to all school login accounts (e.g., Apple ID, computer, Google). You may find that non-compliant passwords will be rejected. As the list of acceptable passwords updates frequently due to leaks or hacks, you may need to try several options. Follow the guidelines below when setting a compliant password.

- 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.

Related Policies

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.

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