

Technology Acceptable Use Policy for Pupils

This policy applies to all pupils attending Stephen Perse Foundation schools.

Here at the Stephen Perse Foundation (the Foundation), 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 Foundation 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:

- 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 Foundation.
- Be aware that any device connected to the SPF 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.
- Respect laws, copyright, personal and privacy rights, age restrictions and intellectual property rights.
- Respect the privacy of others, and in particular not to take or disseminate photos, videos and/or audio recordings of others without the express permission of a member of staff.
- Ensure that your use of IT and online activity both in and out of school does not bring the Foundation 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.
- Be careful with links and attachments in email. If something looks suspicious, do not tap or click on anything within the email, close it and contact the IT Department for further advice.
- 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" network only, with the exception of 1-11 shared school devices.

- 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 Foundation details which are as follows: *The Stephen Perse Foundation, Union Road, Cambridge CB2 1HF - Telephone: 01223 454700.*
- 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, report it to the school immediately. Never leave yourself logged into any device, application or browser unattended or unlocked.
- 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 (ends @appleid.stephenperse.com). The school cannot be held responsible for loss of data stored on SPF systems.
- Ensure any device issued to you or personal device on the school's IT network has the latest critical security updates installed. Personal devices should have up to date antivirus software, be regularly updated, and on an operating system still supported by the manufacturer.
- 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. However, we recognise there may be exceptional circumstances where this is not possible due to regional restrictions, if that is the case please make the school aware.

Disclaimer: Although pupils may be trusted by their parent(s) or guardian with regard to private internet use, the Foundation 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.

School Specific Rules and Information

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 PSHEE, 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.

Years 3 to 6

Technology should only be used in Years 3- 6 with the permission of a member of staff and in accordance with their instructions, activities are closely monitored. 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. Teaching staff direct pupils to recommended websites in lessons and for homework, and they encourage pupils to follow the guidance offered, with regard to safe use of the internet, when they are out of school. Year 6 pupils have a 1:1 provision of iPads in order to prepare them for the Senior School.

Once pupils reach Year 6 they will have the option to take their iPad home at the end of the school day to support their learning, principally through the completion of homework. This is not an expectation but an option for those families where they do not have a personal device at home. 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).

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 like to make people aware it is there as an option.

Years 7 to 13

Two-factor authentication must be enabled on your school Google account, and wherever possible in other systems to protect personal data.

Sixth Form web access is generally not filtered outside of the school unless they are a resident at one of our Boarding Houses. If parents/guardians have any concerns about this please contact the Sixth Form and we can advise. Boarding Houses have enforced curfews for internet access at certain times.

All Senior School, IGCSE One Year Programme and Sixth Form pupils are issued an iPad, protective case, charger, charging lead, access card and lanyard when they join. It is the responsibility of the pupil to keep these items safe. For this reason - regardless of fault - 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. We do not encourage you to arrange your own repairs; only repairs completed by Apple are valid for our warranty.

Charges for damage or replacements

Access card

- 1st loss in an academic year: No charge
- 2nd loss in an academic year: £5
- 3rd and subsequent losses in an academic year: £10
- Lost lanyard: No charge

iPad accessories

- Case replacement if graffitied or damaged: £20
- iPad charger if lost or damaged: £10*
- iPad charging lead if lost or damaged: £10*
- *Note. If you choose to replace the iPad charger and charging lead yourself you must replace them with authentic Apple products.*

iPad

- Grade A - £75: Screen damage (cracks, shattered glass etc).
- Grade B - £150: Damage to the iPad that is beyond a screen replacement. 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.

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. Any equipment provided by the school remains at all times the property of the Foundation and is to be returned on or prior to the last day of your enrollment at the school.

iPads should only be charged with an authentic Apple iPad charger. The protective iPad case must not under any circumstances be damaged or defaced. Any case that requires replacement will be charged as above. Please only use the case that the school provides, and make sure the iPad is kept in it at all times and the cover is closed when not in use.

All school equipment should be returned in good working order with no damage at the end of your use of the equipment, or on leaving the school.

Pupils' Personal Electronic Devices

It is recognised that personal electronic devices, such as mobile phones, are necessary in certain circumstances, e.g. for pupils with long or awkward journeys who may need to contact parents en-route. However, the Foundation 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. Emergency messages from parents for pupils should be sent to Reception and/or the School Office who will pass these on.

Parents are encouraged to ensure that suitable filtering systems are activated on mobile technology used by their child(ren). Pupils are discouraged from using personal electronic devices to gain access to the internet in school. If a personal mobile device contains access to Foundation data, such as school email, it must be protected by a password or fingerprint.

Each Foundation school will have its own rules on mobile phones at school. Please refer to the relevant School Rules for more details.

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 Foundation'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 2018).

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.
- Does not need to be complex (i.e. a combination of upper and lowercase letters/numbers/special characters).
- We recommend at least 3 random words together (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.

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.

Please also refer to:

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

Reviewed: October 2021

=====

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 and Discipline 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. 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.

Student Signature:

Student first name: **Student last name:**

Date:

Version Control

Date of adoption of this policy	7 October 2021
7 October 2021	7 October 2021
Date for next review of this policy	Autumn Term 2022
Policy owner	Director of IT and Head of Rosedale House and Madingley 5-11
Authorised by	Principal, Vice Principal and Heads of Schools