Technology Acceptable Use Policy - 3-11

This policy applies to all pupils attending Stephen Perse Foundation schools between the age of 3-11.

Here at the Stephen Perse Foundation (the Foundation) we recognise the enormous learning potential provided through technology use. 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.

As 3-11 applies to pupils at very different development stages of their lives, we will endeavor to cover below the broad principles that should apply to all:

- 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 anything you post, access or search online or on the school's IT network and devices is filtered in line with government advice, and is traceable and may be monitored and/or logged.
- 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 or videos 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.
- 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.
- Never give out personal or location 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 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 account as best you can, please refer to the 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. 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 so we do not enforce it but like to make people aware it is there as an option.
- Ensure that you regularly 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.
- This will not apply to all but if it does ensure any device issued to you or personal device on the school's IT network has the latest critical security patches installed. Personal devices should have up to date antivirus software where appropriate.
- School email and messaging accounts should only be used for legitimate school related purposes.

Early Years Foundation Stage (EYFS) and KS1 (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.

KS2 (Years 3 to 6)
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. Technology should be used in KS2 only 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 but will not be able to take them off site unless agreed with the Head of School.

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 student'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.

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 school will have its own rules on mobile phones at school. Please refer to their 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 Behaviour and Discipline Policy 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 and would find it difficult to comply with a password policy. Therefore our password policy applies only from Year 3 to Year 6. 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 (eg. 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 (ie. 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.

Passwords will not expire very often. If you suspect someone knows your password, change it immediately.

This policy also applies to iPad passcodes. For Year 6 who have 1:1 iPads, we recommend you set up touch ID so you only have to re-enter the password when you 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 and Discipline Policy - Foundation
- School Rules
- Online Safety Policy - Foundation
- Safeguarding and Child Protection Policy - Foundation

Reviewed: May 2020

Version Control

Date of adoption of this policy	20 May 2020
Date of last review of this policy	20 May 2020
Date for next review of this policy	Summer Term 2021
Policy owner	Director of IT
Authorised by	Vice Principal