Technology Acceptable Use Policy (3-11)

This policy applies to all pupils attending Stephen Perse Foundation (the **Foundation**) schools between the age of 3-11. This includes all children and pupils attending Madingley, Dame Bradbury's and Rosedale House.

This policy refers to all technology including, but not limited to: iPads, PCs and Laptops, Macs, Google Apps, third party apps and mobile phones.

To help ensure full understanding from both pupils and their parents/guardians, Appendix 1, the sign off sheet (at the end of this Policy) requires signing annually by all new and existing parents. Pupils will be asked to sign part of the attached document which will be integrated into their learning as part of their IT lesson.

Guiding Principles

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

Use of technology within the Early Years Foundation Stage (EYFS) and KS1 (Years 1 and 2)

All adults working with pupils within these key stages must adhere to this policy to allow for best use of the technology whilst understanding the potential dangers.

There are opportunities for pupils to use technology, including iPads, during the school day. iPads may be used in lessons and accessed independently in accordance with the Safe Guide to iPad Use which is displayed in all EYFS and KS1 classrooms. Such activities are supervised and monitored. All digital work should be stored in a Stephen Perse Foundation Google Drive account as part of the GSuite for Education domain.

Pupils will have access to the internet through some classroom computers and iPads provided by the Foundation. Pupils are not permitted to use mobile phones in school.

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 directing the pupils through the use of QR codes, Apple Classroom or Google Classroom. Independent research is directly supervised.

Staff may only permit pupils to use technology for electronic communication, such as email, with persons or parties that have previously been authorised by a member of the relevant Senior Leadership Team (SLT). Such communication is directly supervised and only takes place using authorised systems.

stephen perse
foundation

Supervision of technology with internet access in Early Years and KS1 (Years 1 and 2)
Kindergarten, Reception and KS1 use technology in small groups and are independently overseen by members of staff, who have had internet safety training as part of Safer Working Practices. Internet filtering is managed in line with government guidance.

Use of technology within KS2 (Years 3-6)
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. Pupils are made aware of the potential dangers of the internet during PSHEE 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.

There are opportunities for pupils to use the special features of technology, including iPads, during the school day. iPads may be used in lessons with the permission of the member of staff and in accordance with their instructions. Such activities are closely supervised and monitored, and all digital work should be stored in a Foundation Google Drive account as part of the GSuite for Education domain. Appropriate sanctions, as outlined in the 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 pupils without permission
- recording or photographing illegal activity including the downloading, storing or forwarding of indecent images

This list is illustrative rather than exhaustive.

Pupils will have access to a wide variety of apps and software on school devices, some of which require signing in. Pupils must never give out personal information about themselves or others without first discussing with a parent or guardian.

stephen perse
foundation

Pupils Personal Electronic Devices

The Foundation cannot take responsibility for loss or damage to pupils' personal electronic devices. They should not be left unattended in school, e.g. in bags or table trays. Parents should be aware of the potential risks for children of using technology such as theft, bullying and inappropriate contact, including grooming by unsuitable persons. Parents are encouraged to ensure that suitable filtering systems are activated on technology used by their child(ren).

Emergency messages from parents for pupils should be directed to the relevant School Office. It is recognised that mobile devices are necessary in certain circumstances, e.g. for pupils' journeys to and from school. Under these circumstances technology may be switched on and used outside normal school hours. All mobile devices should be switched off and handed in to the School Office and collected only at the end of the school day.

Pupils must seek the permission of a member of staff before using personal electronic devices on Foundation premises, activities and trips; this includes taking photographs and making recordings.

If a personal electronic device is activated during school hours, without the permission of a member of staff, it will be confiscated for the rest of that school day. Staff will take confiscated devices to the School Office and the Head of School will be informed.

Searching screening and confiscation

Pupils' 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 School 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 School Rules.

If an electronic device that is prohibited by the School 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 of the incident is kept, including the reasons for the search and its outcome.

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

Access to the web outside of the school may be directed through the schools web filtering system. Access through the schools filtering system results in the collection of web history and IP address information. This may be monitored by staff and investigated if inappropriate or concerning online behaviour is detected/suspected. The Foundation uses industry approved filtering and monitoring systems in line with Keeping Children Safe in Education (KCSIE) guidelines. Whilst these systems are very effective in guarding against inappropriate content, there is always the possibility of something you would expect to be blocked getting through. The Foundation cannot be held responsible in these instances and is not accountable for students visiting inappropriate content whilst using the internet outside of the Foundations systems.

Further information and guidance can be found here:
https://www.saferinternet.org.uk/advice-centre/young-people

Please refer to:

- Anti-Bullying Policy – Foundation
- Behaviour and Discipline Policy – Foundation
- Cameras, Mobile Phones and Pupil Information - Pre-Prep
- Online Safety Policy - Foundation
- Safeguarding and Child Protection Policy - Foundation
- Safe iPad Use in Class Poster - Pre-Prep Classrooms
- School Rules – Pre-Prep/Junior School/Dame Bradbury's

Reviewed: June 2019

stephen perse foundation

Version Control

Date of adoption of this policy	1 July 2019
Date of last review of this policy	26 June 2019
Date for next review of this policy	Summer Term 2020
Policy owner	IT Manager
Authorised by	Operations FLT and Heads of Schools

stephen perse
foundation

Appendix 1
Agreement to the Technology Acceptable Use Policy (3-11)

==========

I have read the Technology Acceptable Use Policy (3-11) 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.

Pupil Signature: .....

Pupil first name: ..... Pupil last name: .....

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

Date: .....

I have read in full the Technology Acceptable Use Policy (3-11) attached and agree to help ensure my child abides by this policy.

PARENT/GUARDIAN Name: .....

PARENT Signature: .....

Date: .....