

THE SOCIETAS TRUST

Pupils' Personal Electronic Devices Policy

Date of Policy	2026
Reviewed and Agreed by	The Directors' Board
Review Date	16 September 2026
Next Review Date	Autumn 2027

Contents:

Statement of intent

1. Legal framework
2. Roles and responsibilities
3. Ownership and responsibility
4. Acceptable use
5. Unacceptable use
6. Cyberbullying
7. Searching pupils
8. Accessing and storing data
9. Sanctions

Appendices

A. Device and Technology Acceptable Use Agreement for Pupils

Statement of intent

Mobile phones, tablets and other personal electronic devices have become widely available and accessible to pupils.

The Societas Trust accepts that personal mobile phones and tablets are often given to pupils by their parents to ensure their safety and personal security, but understands that such devices pose inherent risks and may jeopardise the learning environment.

We must strike a balance between personal safety and a suitable educational setting. We understand that parents may wish for their child to carry a mobile phone for their personal safety, whilst pupils may wish to bring additional devices to school for other reasons. This policy establishes how personal electronic devices should be used by pupils in school to ensure both personal safety and an appropriate learning environment.

Personal electronic devices include, but are not limited to the following items:

- Mobile phones
- Personal digital assistants (PDAs)
- Handheld entertainment systems, e.g. video game consoles, iPods
- Portable internet devices, e.g. tablets, laptops
- Wireless handheld technologies or portable information technology systems, e.g. devices used for word processing, wireless internet access, image capture and/or recording, sound recording, and information transmitting, receiving and/or storing

1. Legal framework

This policy has due regard to all relevant legislation and statutory and good practice guidance including, but not limited to, the following:

- DfE (2024) 'Mobile phones in schools'
- DfE (2024) 'Behaviour in Schools'
- DfE (2025) 'Keeping children safe in education 2025'
- DfE (2023) 'Searching, screening and confiscation at school'
- Data Protection Act 2018
- The UK General Data Protection Regulation (UK GDPR)
- Voyeurism (Offences) Act 2019
- Protection of Children Act 1978
- Sexual Offences Act 2003
- DfE (2014) 'Cyberbullying: Advice for headteachers and school staff'

This policy operates in conjunction with the following school policies:

- Anti-bullying Policy
- Online Safety Policy
- Data Protection Policy
- Data Retention Policy
- Safeguarding and Child Protection Policy
- Complaints Policy
- Social Media Policy
- Child-on-Child Abuse Policy
- Behaviour Policy
- Code of Conduct for Adults

The new government guidance states that schools should:

- Prohibit the use of mobile phones and other smart technology throughout the school day, this includes during lessons, between lessons, breaktimes and lunchtime.
- Develop and implement a tailored policy on the use of mobile phones and other similar devices in school.

2. Roles and responsibilities

The Governing Board will be responsible for:

- The implementation of the policy and procedures.
- Evaluating the effectiveness of the policy and procedures.
- Ensuring that the policy, as written, does not discriminate on any grounds.
- Reviewing the policy annually.

The headteacher will be responsible for:

- Handling complaints regarding this policy as outlined in the school's Complaints Procedures Policy.

- The day-to-day implementation and management of the policy.
- Informing parents and pupils of the Personal Electronic Devices Agreement.
- Communicating this policy to the relevant staff members and the wider school community.
- Communicating what devices can be brought to school and when they can and cannot be used.

Staff members will be responsible for:

- Negotiating incidents of cyberbullying in conjunction with the headteacher, in line with the Anti-bullying Policy and the Behaviour Policy.

The DSL will be responsible for:

- Initiating and managing responses to incidents with relevant staff members and in line with the Safeguarding and Child Protection Policy.
- Liaising with and reporting the relevant information to children's social care and/or the police, when it is necessary to do so.

Pupils are responsible for adhering to the provisions outlined in this policy.

3. Ownership and responsibility

Pupils are responsible for their own belongings. The school accepts no responsibility for replacing property that is lost, stolen or damaged either on school premises or travelling to and from school, and at school events.

Staff will be protected against liability in any proceedings brought against them for any loss or damage to personal devices that have been confiscated as an appropriate sanction, provided that they have acted lawfully.

Pupils are responsible for replacing school property they lose, damage or steal, including electronic devices.

Pupils should enable a personal PIN or passcode on all the approved devices brought to school to protect their personal data, images and videos in the event that the device is lost, stolen or accessed by an unauthorised person.

4. Acceptable use

Pupils should request permission from the headteacher before using personal devices during school hours (this excluded mobile phones which are not permitted as the school is a mobile free environment).

The mobile free environment is achieved by:

- Ensuring that mobile phones are handed in on arrival – phones will be returned to pupils at the end of the school day

The school will make reasonable adjustments for pupils to use their mobile phones in specific circumstances, e.g. to monitor a medical condition via an app or if they are a young carer.

5. Unacceptable use

Pupils will not be permitted to use their mobile phones in school at any time – this includes in between lessons and during break and lunchtimes. The school will, however, consider if pupils should have access to their devices on the way to and from school where access might be required for personal safety reasons.

Whilst on the school grounds, when children are arriving and leaving school, unless express permission is granted by a member of staff, mobile devices will not be used to perform any of the following activities:

- Make phone or video calls
- Send text messages, WhatsApp messages, iMessages or emails
- Access social media
- Play games
- Watch videos
- Take photographs or videos
- Use any other application during school lessons and other educational and pastoral activities

Pupils will adhere to the Social Media Policy at all times.

Files will not be sent between mobile devices, and Bluetooth and Wi-Fi functions will be disabled while on school premises.

Personal electronic devices will not be plugged into outlets on the school premises without the express permission of the headteacher, and they will have an up-to-date portable appliance test (PAT).

Staff will not give out their personal contact details to pupils. If correspondence is needed between staff members and pupils for homework or exams, staff should provide their school contact details.

Under the Voyeurism (Offences) Act 2019, the act known as “upskirting” is an offence. Any incidents will not be tolerated by the school. Despite the name, anyone (including both pupils and teachers) of any gender, can be a victim of upskirting.

A “specified purpose” is namely:

- To humiliate, distress or alarm the victim

Any incidents of upskirting will be reported to the DSL and handled in accordance with the school’s Safeguarding and Child Protection Policy.

6. Cyberbullying

Incidents of cyberbullying will be dealt with and reported in line with the Anti-bullying Policy and the Behaviour Policy.

As part of the school's ongoing commitment to the prevention of cyberbullying, regular teaching and discussion about online safety will take place as part of PSHE lessons.

7. Searching pupils

School pupils have a right for their private life to be respected under article 8 of the European Convention on Human Rights (ECHR). This right is not absolute, and the school can interfere with this right as long as it is justified, proportionate, and aligns with the powers to search in the Education Act 1996.

All searches will be conducted in line with the school's Searching, Screening and Confiscation Policy.

The headteacher, and other authorised staff members, will have the power to search a pupil or their possessions where they have reasonable grounds to suspect that a pupil is in possession of a prohibited item. Mobile phones and similar devices will be deemed as prohibited items that may be searched for in line with the Behaviour Policy.

In all cases the authorised member of staff will always:

- Seek the co-operation of the pupil before conducting a search.
- Ensure the pupil understands the reason for the search and how it will be conducted.
- Give the pupil the opportunity to ask any questions so that their agreement is informed.
- Have due regard to the DfE's 'Searching, screening and confiscation' guidance.

Staff may search a pupil's outer clothing, pockets, possessions, desks or lockers. Staff conducting a search must not require the pupil to remove any clothing other than outer clothing - outer clothing means any item of clothing that is not worn wholly next to the skin or immediately over a garment that is being worn as underwear and includes hats, shoes, boots or scarves. Possessions means any goods over which the pupil has or appears to have control - this includes desks, lockers and bags.

A staff member may ask a pupil to show them what they are doing on their mobile phone or tablet if they reasonably believe that the pupil is using the device to cause harm. If it is judged reasonable, the staff member may inspect the files or data on a pupil's electronic device and delete them if necessary.

Staff members will ensure they have a good reason to examine and delete data on a pupil's electronic device. When determining a good reason to examine data, staff members will ensure they reasonably suspect that the data has been, or could be, used to cause harm, undermine the safe environment of the school and disrupt teaching, or be used to commit an offence.

When determining a good reason to delete data, staff members will consider whether the material found may constitute evidence relating to a suspected offence and if so, choose not

to delete the data. The data may be deleted if it is found likely to cause harm to any person, and the pupil and/or parent refuses to delete the data themselves.

If a search uncovers a device that is being used to cause harm, or which contains prohibited material such as pornography, a staff member can confiscate the device. If a staff member finds child pornography, it must be given to the police as soon as reasonably practicable. Where staff find stolen items like mobile devices, they must be given to the police as soon as reasonably practicable.

The staff member conducting the search must be the same sex as the pupil being searched. A witness to the search must be present; this should also be a staff member of the same sex as the pupil being searched.

Pupils are required to comply with any request to check their electronic device.

Pupils are required to comply with any request to disable the screen lock function of their electronic device and show any staff member what they are doing. Any pupil who refuses to comply with these requests will be disciplined in line with the Behaviour Policy.

8. Accessing and storing data

Downloading and accessing inappropriate websites and data on school-owned electronic devices is strictly prohibited.

Storing and using the personal data of any pupil or member of staff for non-work-related activity is strictly prohibited.

All data access requests will be handled in line with the school's Data Protection Policy.

9. Sanctions

Using a personal electronic device is a privilege which can be revoked at any time. Any pupil caught acting in a manner that contradicts this policy will have their personal electronic device confiscated until the end of the day.

Confiscated personal electronic devices will be locked away securely. Confiscated personal electronic devices will be collected by the pupil's parent.

Bullying via personal electronic devices will be dealt with in line with the school's Anti-bullying Policy.

Appendix A: Device and Technology Acceptable Use Agreement

At **Summerbank Primary School**, we know that using technology is an important part of your learning experience. We want everyone to be able to use technology, like the internet and laptops, but it is important that you are safe when you are using technology.

This agreement will set out the rules around using technology and devices, such as laptops and phones, when you are at school. Parents/carers are asked to share this document carefully with their child.

If you have any questions about anything in this agreement, speak to your **teacher**.

Definitions

Before you read the agreement, here are some key terms you should understand:

- **Technology** – this includes any ICT systems at the school, including the internet.
- **School-owned devices** – any devices that are owned by the school that have been given to you to help with your school work, including laptops and tablets.
- **Personal devices** – any device that belongs to you that you bring into school, including mobile phones.

Security and protecting information

I will:

- Make sure I understand what I can do to keep my information safe when using technology and devices – I will speak to my **teacher** if I have any questions.

I will not:

- Try to get around any security measures the school has put in place on the internet or school-owned devices.
- Share any of my passwords with other people.

Using technology in school

I will:

- Only use technology and devices that I have been given permission to use.
- Only access websites, apps and other online platforms that I have been given permission to use.
- Only use the school's ICT facilities, technology and devices to complete schoolwork.
- Only go on the internet for something other than schoolwork during break and lunch times.

I will not:

- Install any software onto school ICT systems unless I have been told to do so by a member of school staff.
- Search for, view, download, upload or send anything inappropriate when using the internet.

Emails

I will:

- Only use the email account that has been set up for me by the school when sending emails related to my schoolwork.

I will not:

- Open any emails from people I do not know.
- Use my personal email address for schoolwork, unless I have been told I can do so by a member of school staff.

School-owned devices

I will:

- Only use school-owned devices to carry out my schoolwork.
- Only use websites and apps that a member of staff has said I can use.
- Understand that the school will monitor how I use school-owned devices.
- Take care of school-owned devices when I am using them.
- Tell a member of staff if a school-owned device is damaged or lost when I am using it.
- Tell a member of staff if I think something has happened in relation to the security of the device, e.g. if I download an attachment from an email from someone I do not know.

I will not:

- Use school-owned devices to send inappropriate messages, images, videos or other content.
- Use school-owned devices to view, store, download or share any inappropriate, harmful or illegal content.
- Use school-owned devices to go on personal social media accounts.

Personal devices

I will:

- Understand that if my personal devices are lost, damaged or stolen, it is not up to the school to pay for any costs.

I will not:

- Use my personal device or mobile phone in school at any time – this includes in between lessons, during break and lunchtimes, whilst on the school grounds, when arriving and leaving school, unless express permission is granted by a member of staff.
- Use my personal devices to send inappropriate messages, images, videos or other content.

- Use my personal devices to view, store, download or share any inappropriate, harmful or illegal content.

Social media

I will:

- Think about what I post about the school on social media and make sure I do not post anything that could be harmful to any member of the school community.

I will not:

- Try to speak to any member of staff on social media.
- Accept or send 'friend' or 'follow' requests from members of staff on social media.
- Send any abusive, threatening or otherwise inappropriate messages on social media.
- Bully anyone through social media.

Reporting misuse

I will:

- Understand that my use of the internet will be monitored by the **ICT technician** and recognise the consequences if I do not follow this agreement.
- Understand that the **headteacher** may decide to take disciplinary action against me, in accordance with the **Behaviour Policy**, if I do not follow this agreement.