Springcroft Primary School

Electronic Devices Policy

Date Adopted: September 2025
Author/owner: Springcroft Primary School
Anticipated Review: Autumn Term 2026

Approved	Signature	Date

Our Mission Statement:
The place to learn, the place to succeed, the place to make friends, the place to grow.

Contents

Introduction and Aims

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

At Springcroft Primary School the welfare and well-being of our pupils is paramount. The aim of this policy is to allow users to benefit from modern communication technologies, whilst promoting safe and appropriate practice through establishing clear and robust acceptable device user guidelines. This is achieved through balancing protection against potential misuse with the recognition that electronic devices are effective communication tools. It is recognised that it is the enhanced functions of many electronic devices that cause the most concern, offering distractions and disruption to the working day, and which are most susceptible to misuse, including using AI that may have an impact on academic integrity and its potential for misuse, the taking and distribution of indecent images, exploitation and bullying. However, as it is difficult to detect specific usage, this policy refers to ALL mobile communication devices able to take pictures, record videos, send or receive calls and messages. This includes cameras, mobile telephones, tablets and any recording devices including smartwatches. More and more devices are technically capable of connecting us to the outside world. We will adapt the policy to include all devices we deem required to safeguard children and staff.

As a school, 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, while 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
- 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
- Smart watches
- Smart glasses

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 ‘Mobile phones in schools’
- DfE ‘Behaviour in Schools’
- DfE ‘Keeping children safe in education 2025’

- DfE ‘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 ‘Cyberbullying: Advice for Headteachers and school staff’

This policy operates in conjunction with the following school policies:

- Anti-bullying Policy
- Online Safety Policy
- GDPR Policy
- Safeguarding Policy
- Complaints Procedures Policy
- Child-on-child Abuse Policy
- Mental Health, Wellbeing and Behaviour for Learning Policy
- Staff Code of Conduct Policy

Code of conduct

A code of conduct is promoted with the aim of creating a cooperative school community, where all stakeholders work as a team, have high values and respect each other; thus creating a strong morale and sense of commitment leading to increased productivity. Our aim is therefore that all practitioners:

- have a clear understanding of what constitutes misuse
- know how to minimise risk.
- avoid putting themselves into compromising situations which could be misinterpreted and lead to possible allegations.
- understand the need for professional boundaries and clear guidance regarding acceptable use.
- are responsible for self-moderation of their own behaviours.
- are aware of the importance of reporting concerns promptly.

It is fully recognised that imposing rigid regulations on the actions of others can be counterproductive. An agreement of trust is therefore promoted regarding the carrying and use of mobile phones within the setting, which is agreed to by all users.

Acceptable use

This policy applies to any computer or other device connected to the school's network and computers, be it a school provided device or a personal device.

The school will monitor the use of all ICT facilities and electronic devices that are the property of the school. Members of staff will only use school-owned and approved personal devices for work duties and educational purposes. The duties for which use is permitted include, but are not limited to, the following:

- Preparing work for lessons, activities, meetings, reviews, etc.
- Researching any school-related task
- Any school encouraged tuition or educational use
- Collating or processing information for school business.
- Communicating with other members of staff, such as contacting the school office for assistance.

Inappropriate use of school-owned and personal devices could result in a breach of the school's GDPR Policy and a breach of legislation, including the UK GDPR and Data Protection Act 2018. Any member of staff found to have breached the school's GDPR Policy or relevant legislation will face disciplinary action.

School-owned electronic devices will not be used to access any material which is illegal, inappropriate, or may cause harm or distress to others. Any illegal, inappropriate or harmful activity will be immediately reported to the headteacher.

Staff will always be an example of good practice to pupils, serving as a positive role model in the use of ICT and related equipment.

Staff, children and Governors will not:

- Open email attachments from unknown sources.
- Use programmes or software that may allow them to bypass the filtering or security systems.
- Upload or download large capacity files without permission from the ICT technician.
- Give their home address, phone number, social networking details or email addresses to pupils or parents – contact with parents will be done through authorised school contact channels.
- Take their allocated classroom mobile phone out of the school premises, unless permitted by the headteacher.

All data will be stored appropriately in accordance with the school's GDPR Policy. Members of staff will only use school-owned electronic devices to take pictures or videos of people who have given their consent. School-owned electronic devices will not be used to access personal social media accounts. Personal electronic devices will not be used to communicate with pupils or parents, including via social media.

Staff will ensure they:

- Express neutral opinions when representing the school online.
- Avoid disclosing any confidential information or comments regarding the school, or any information that may affect its reputability.
- Have the necessary privacy settings are applied to any social networking sites.

Images or videos of pupils, staff or parents will only be published online for the activities for which consent has been sought.

Copyrighted material will not be downloaded or distributed.

School-owned devices will be taken home for work purposes only, once approval has been sought from the Headteacher and ICT technician. Remote access to the school network will be given to staff using these devices at home. School equipment that is used outside the premises, e.g. laptops, will be returned to the school when the employee leaves employment, or if requested to do so by the Headteacher. While there is scope for staff to utilise school equipment for personal reasons, this will not be done during working hours unless approved by the Headteacher or in the case of a personal emergency. Private business will not be mixed with official duties, e.g. work email addresses will be reserved strictly for work-based contacts only.

Personal use of school-owned equipment can be denied by the Headteacher at any time. This will typically be because of improper use or over-use of school facilities for personal reasons. A charge may be made for using equipment if the values are significant. Where permission has been given to use the school equipment for personal reasons, this use will take place during the employee's own time, e.g. during lunchtime or after school. Where this is not possible, or in the case of an emergency, equipment can be used for personal reasons during work hours provided that disruption to the staff member's work, and the work of others, is minimal.

Abuse of ICT facilities or devices could result in privileges being removed. Staff will be aware of acceptable ICT use, and misuse of the facilities, as defined in this policy, will be reported to the Headteacher. Failure to adhere to the rules described in this policy may result in disciplinary action, in line with the Disciplinary Policy and Procedure.

Pupils will ensure they:

Pupils bringing personal electronic devices into school must make their parents aware of this.

Personal electronic devices will be switched off and left in the school office during the school day unless the pupil is using the device as part of a lesson with the permission of their class teacher.

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.

Pupils may use their onedrive account to transfer schoolwork from the school premises to their home. All staff members will adhere to the GDPR Policy when sending work home with pupils.

Unacceptable use

Personal electronic devices will not be used in any manner or place that is disruptive to the normal routine of the school. Unless express permission is granted by a member of staff, mobile devices will not be used to perform any of the following activities whilst on school grounds:

- 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 not be permitted to use their mobile phones throughout the course of the school day – this will include in between lessons and during break and lunchtimes. The school will, however, consider the risks that may be posed to pupils who do not have access to their mobile phone, e.g. when organising travel home at the end of the school day.

Staff members will also not be permitted to use their mobile phone for personal reasons in front of pupils throughout the school day.

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

If pupils fall ill during school hours, they will not use their mobile device to contact parents. The school office will contact parents direct.

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:

- Obtaining sexual gratification (either for themselves or for the person they are enabling to view the victim’s genitals, buttocks or underwear)
- 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 Child Protection and Safeguarding Policy.

Personal Electronic Devices, Mobiles, Smart Watches, Smart Glasses - Staff

- Staff are not permitted to make/receive calls/texts during contact time with children. Emergency contact should be made via the school office.
- Staff should have their phones switched to silent or off and out of sight (e.g. in a drawer, handbag or pocket) during class time. Staff may choose to leave their phones in their pigeon holes located in the staff room. Mobile phones and personal electronic devices including communicating using a smart watch should not be used in a space where children are present (e.g. classroom, playground).
- Use of phones and smart watches (including receiving/sending texts and emails) should be limited to non-contact time when no children are present e.g. in office areas, staff room, empty classrooms.
- It is also advised that staff protect access to functions of their phone and devices.
- Should there be exceptional circumstances (e.g. acutely sick relative), then staff should make the Headteacher aware of this and can have their phone in case of having to receive an emergency call.
- Staff are not at any time permitted to use recording equipment on their mobile phones, for example: to take recordings of children, or sharing images. Legitimate recordings and photographs should be captured using school equipment such as the school iPad. Staff may wish to consider the use of a camera block app that prohibits the operation of a devices camera between a specified time and logs this.
- Staff should report any usage of any electronic devices that causes them concern to the Headteacher.
- In the event of an emergency lockdown staff should retrieve their phones at the earliest opportunity as this will be a means in which communication may well be made.

Mobile Phones for work related purposes

We recognise that mobile phones provide a useful means of communication on offsite activities. However, staff should ensure that:

- Mobile use on these occasions is appropriate and professional (and will never include taking photographs of children).
- Mobile phones should not be used to contact parents during school trips – all relevant communications should be made via the school office during the school operating hours or via an SLT member outside of normal working hours.
- Where parents are accompanying trip's, they are informed not to contact other parents (via calls, text, email or social networking) during the trip or use their phone to take photographs of children.

Personal Mobiles, Smart Watches, Smart Glasses - Pupils

We recognise that mobile phones are part of everyday life for many children and that they can play an important role in helping pupils to feel safe and secure. However, we also recognise that they can prove a distraction in school and can provide a means of bullying or intimidating others. Therefore:

- Pupils are not permitted to have mobile phones in school or on trips unless specific permission is granted by the visit leader.
- If in the rare event of a parent wishing for his/her child to bring a mobile phone to school to contact the parent after school, then parents should first fill a consent form agreeing to the school's conditions of use policy (See Appendix 1). The phone must be handed in, switched off, to the school office first thing in the morning and collected from them by the child at home time (all devices are stored securely).
- Mobile phones brought to school without permission will be confiscated and returned at the end of the day.
- The use of Smart Watches is not appropriate in school due to risks of loss and damage and of misuse in the same way as mobile phones or tablets.
- The use of personal Smart Watches and Smart Glasses by pupils is prohibited throughout the school day, as these devices have similar functionality to mobile phones (e.g., communication, recording, internet access). Any such device must be removed and will be stored securely by staff for the duration of the school day.

Where mobile phones are used in or out of school to bully or intimidate others, then the Headteacher does have the power to intervene to such an extent as it is reasonable to regulate the behaviour of pupils when they are off the school site.

Electronic Devices in the EYFS

All personal electronic devices including mobile phones and smart watches must be stored securely out of reach within the setting during contact time with children. (This includes staff, visitors, parents, volunteers and students). No parent is permitted to use their mobile phone or use its camera facility whilst inside school buildings beyond the school entrance hall.

Portable Appliance Testing (PAT)

Personal electronic devices that require charging or plugging into the mains are not permitted on school premises unless they have passed Portable Appliance Testing (PAT). This ensures any personal item, such as laptops, tablets, or chargers brought in for educational use, meets necessary electrical safety standards.

Sanctions

When allowed during school time, using a personal electronic device is a privilege which can be revoked at any time. Any staff member, pupil, visitor or Governor 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 in the school's admin office. Confiscated personal electronic devices will be collected from the school office and the pupil's parent will be contacted to inform them of the confiscation. In repeat incidents of staff or children using personal devices inappropriately, the Headteacher will determine the length of time they deem proportionate for confiscation.

Searching and Data

The Headteacher, and staff members authorised by the Headteacher, have the power to search a pupil or their possessions without consent if they have reasonable grounds for suspecting that the

pupil is in possession of a banned item, or an item that has been, or is likely to be, used to commit an offence, cause personal injury or damage to property.

Data Access and Deletion

Where a mobile phone or other electronic device is confiscated, the Headteacher, or staff authorised by them, has the statutory power to examine any data or files on the device if they reasonably suspect the data/file relates to a criminal offence, or may be used to cause harm, disrupt teaching, or break school rules. The school may also delete or erase any file or data if there is a good reason to do so, unless it is evidence of a criminal offence (in which case it must be handed to the police.

Any material found during a search that is suspected to be evidence of a criminal offence (e.g., child sexual abuse images or extreme pornography) will not be deleted and will be passed immediately to the Designated Safeguarding Lead (DSL) who will involve the police as soon as reasonably possible.

Volunteers, Visitors, Governors and Contractors

All Volunteers, Visitors, Governors and Contractors are expected to follow this policy as it relates to staff whilst on the premises. On arrival, such visitors will be informed of our expectations around the use of mobile phones and electronic devices.

Parents

We understand that many parents see their phones as essential means of communication at all times. Therefore, we ask that parents' usage of mobile phones, whilst on the school site is courteous and appropriate to the school environment. If a parent needs to make a call whilst attending a school event, then we ask that this is done in the school entrance hall or outside of the school building.

However, if family members do wish to take photographs or video with their own cameras/ electronic devices during a performance, or indeed during any other school event, the school will only permit this, providing that the following ground rules are adhered to in order to respect others and ensure safeguarding is not compromised:

Cyberbullying

All personal electronic devices will be used in line with our Online Safety Policy.

The school will sanction pupils for online behaviour (including cyberbullying or misuse of electronic devices) that takes place outside of school hours or off school premises, if that behaviour causes harm to another pupil, affects the orderly running of the school, or adversely affects the reputation of the school. Incidents of cyberbullying will be dealt with and reported in line with the Anti-bullying Policy and the Mental Health, Wellbeing and Behaviour for Learning 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.

Accessing and storing data

Cloud-based storage

Data held in remote and cloud-based storage is still required to be protected in line with the UK GDPR and DPA 2018; therefore, members of staff will ensure that cloud-based data is kept confidential and no data is copied, removed or adapted

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

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

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

Removeable media, such as USB drives, DVDs and CDs are not permitted in school.

Sporting events, concerts, productions and other performance events:

- As an invited guest of the school ensure that you follow their requests as to when and where you can safely take photographs of your own child. This will usually be at the end of an event and only in a particular area.
- Ensure that any and all images taken at school events are exclusively for personal use and are not uploaded to the internet, posted on social networking sites or openly shared in other ways.
- Refrain from taking further photographs and/or video if and when requested to do so by staff.

As noted above, it may be necessary for the school to request that no photography or filming take place at a school event (for example, to account for specific safeguarding needs). In such circumstances, this restriction will, as far as possible, be made clear to all those attending before the event begins. Anyone who continues to take photographs, video or other images after being informed of such a restriction will be asked by a member of staff to stop and to delete any material they have recorded. Where photographs and/or videos are taken by parents, guardians, grandparents or other family members, then we ask that parents do not publish images (e.g. on social networking sites) that include any children other than their own.

Safety and security

The school's network will be secured using firewalls in line with the Data and Cyber-security Breach Prevention and Management Plan. Filtering of websites, as detailed in the Data and Cyber-security Breach Prevention and Management Plan, will ensure that access to websites with known malware are blocked immediately and reported to the ICT technician.

Approved anti-virus software and malware protection will be used on all approved devices. The school makes use mail security technology to detect and block any malware transmitted via email.

Members of staff will ensure that all school-owned electronic devices are made available for anti-virus updates, malware protection updates and software installations, patches or upgrades, as required.

Programmes and software will not be installed on school-owned electronic devices without permission from the ICT technician. Staff will not be permitted to remove any software from a school-owned electronic device without permission from the ICT technician. Members of staff who install or remove software from a school-owned electronic device without seeking authorisation from the ICT technician, may be subject to disciplinary measures.

All devices will be secured by a password or biometric access control. Staff and pupils are encouraged to enable a personal PIN or passcode on all the devices they bring 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. Passwords will be kept confidential and must not be shared with pupils, unauthorised members of staff or third parties. Devices should be configured so that they are automatically locked after being left idle for a set time. All devices must be encrypted using a method approved by the DPO.

Loss, theft and damage

Staff, pupils and visitors 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.

For the purpose of this policy, "damage" is defined as any fault in a school-owned electronic device caused by the following:

- Connections with other devices, e.g. connecting to printers which are not approved by the ICT technician
- Unreasonable use of force
- Abuse
- Neglect
- Alterations
- Improper installation

Staff, pupils and visitors are responsible for replacing school property they lose, damage or steal, including electronic devices.

The school's insurance will cover school-owned electronic devices that are damaged or lost, during school hours, if they are being used in relation to school matters. However, staff members will use school-owned electronic devices within the parameters of the school's insurance cover – if a school-owned electronic device is damaged or lost outside of school hours and/or off-site, the member of staff at fault may be responsible for paying damages.

Any incident that leads to a school-owned electronic device being lost will be treated in the same way as damage. The ICT technician and Headteacher will decide whether a device has been damaged due to the actions described above. The ICT technician will be contacted if a school-owned electronic device has a technical fault.

If it is decided that a member of staff is liable for the damage, they will be required to pay a percentage of the total repair or replacement cost. A written request for payment will be submitted to the member of staff who is liable to pay for damages. If the member of staff believes that the request is unfair, they can make an appeal to the Headteacher, who will make a final decision within two weeks. In cases

where the Headteacher decides that it is fair to seek payment for damages, the member of staff will be required to make the payment within six weeks of receiving the request. Payments will be made to the school via the main office, and a receipt is given to the member of staff. The school will accept payments made via credit and debit cards, bank transfer and cash. A record of the payment will be made and stored in the main office for future reference. The Headteacher may accept the payment in instalments. If the payment has not been made after six weeks, the fee will increase by five percent and continues for a maximum of six months – at which point formal disciplinary procedures will begin.

The member of staff will not be permitted to access school-owned electronic devices until the payment has been made. In cases where a member of staff repeatedly damages school-owned electronic devices, the headteacher may decide to permanently exclude the member of staff from accessing devices.

If a school-owned device is lost or stolen, or is suspected of having been lost or stolen, the DPO will be informed as soon as possible to ensure the appropriate steps are taken to delete data from the device that relates to the school, its staff and its pupils, and that the loss is reported to the relevant agencies. The school will not be responsible for the loss, damage or theft of any personal device, including phones, cameras, tablets, removable media, etc.

.

Appendix 1 - Mobile Phone Parental consent form

We do not believe that pupils require access to mobile phones at school. However, we do acknowledge that some parents/carers may consider that their child needs to bring a phone into school because of special circumstances e.g. walking to or from school without adult supervision or going home with another parent etc.

Phones should only be brought in for children in Years 5 and 6.

If you wish for your child to bring their mobile phone into school then please can you complete the consent and conditions of use form below.

Conditions of use

The phone will not be switched on within the school building or grounds.

The phone must be handed into the school office as soon as your child arrives at school.

The school bears no responsibility for the loss or damage to any electronic device bought into school.

Should your child be found using their phone inappropriately, the school reserves the right to withdraw this privilege and they will no longer be able to bring the phone into school.

If you have any queries regarding this please speak to the school office in the first instance.

Name of child	
Child's class	
Make and model of mobile phone	
Parents signature	