Mobile and Smart Technology Policy

King David PRIMARY SCHOOL & NURSERY

Approved by: Curriculum Committee	**Date: 11/11/2026**
Last reviewed on:	
Next review due by:	**November 2028**

Contents

1 - Policy aims and scope 3
2 - Links with other policies 3
3 - Safe use of mobile and smart technology expectations 3
4 - School provided mobile phones and devices. 4
5 - Staff use of mobile and smart technology 4
5.1 Staff Smart watches 5
6 - Pupil's use of mobile and smart technology 6
6.1 Pupil use of smartwatches 7
7 - Visitors' use of mobile and smart technology 7
8 - Emerging online risks 7
9 - Policy monitoring and review 8
10 - Responding to policy breaches 8

1 - Policy aims and scope

- The purpose of this policy is to safeguard and promote the welfare of all members of the King David school when using mobile devices and smart technology. This policy applies to all school activity including in school and on educational visits and when school devices are used by staff or pupils away from the school site.

  - King David Primary School recognises that online safety is an essential part of safeguarding and acknowledges its duty to ensure that all pupils and staff are protected from potential harm when using mobile and smart technology.

    As outlined in our Child Protection Policy, the Designated Safeguarding Lead (DSL), Nina Capek is recognised as having overall responsibility for online safety.
- This policy applies to all who have access to and use mobile and smart technology on site; this includes mobile phones and personal devices such as tablets, e-readers, games consoles and wearable technology, such as 'smart watches and fitness trackers, which facilitate communication or have the capability to record sound or images.
- This policy applies to pupils, parents/carers and all staff, including the governing body, leadership team, teachers, support staff, external contractors, visitors, volunteers and other individuals who work for, or provide services on behalf of the setting (collectively referred to as "staff" in this policy).

2 - Links with other policies

- This policy links with several other policies, practices, and action plans, including but not limited to:

  - DFE mobile phones in schools statutory guidance
  - Anti-bullying policy
  - Acceptable Use Policies (AUP)
  - Behaviour policy
  - Child protection policy
  - Code of conduct/staff behaviour policy
  - Curriculum policies, such as: Computing, Personal Social and Health Education (PSHE), Citizenship and Relationships and Sex Education (RSE)
  - Online Safety Policy

3 - Safe use of mobile and smart technology expectations

King David Primary School recognises that use of mobile and smart technologies is part of everyday life for many pupils , staff, and parents/carers.

- Electronic devices of any kind that are brought onto site are the responsibility of the user. All members of King David are advised to:

- take steps to protect their mobile phones or personal devices from loss, theft, or damage; we accept no responsibility for the loss, theft or damage of such items on our premises.
- use strong passwords/PIN numbers to ensure that unauthorised access, calls or actions cannot be made on their phones or devices. A strong password is at least 8 characters and include numbers, upper case and a special character.

- Mobile phones and personal devices are not permitted to be used throughout the school day unless this is on their own break/lunch time or have permission from the head teacher.
- The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the community, any breaches will be dealt with in line with our anti- bullying, behaviour, and child protection policies.
- All members of King David are advised to ensure that their mobile phones and personal devices do not contain any content which may be offensive, derogatory, or illegal, or which would otherwise contravene our behaviour or child protection policies.

4 - School provided mobile phones and devices.

- Members of staff will be issued with a mobile phone and/or mobile device in addition to their work email address, where it is a necessary requirement for them to do their job. Depending on roll and need these will be provided by the school and remain the property of the school. This could be : A laptop, A tablet, A Mobile phones - need will be determined by the Headteacher and supported by IT technician.
- School provided mobile phones and devices must be suitably protected via a strong password/PIN and must only be accessed by the individual it is given to. A strong password is defined as one that is at least 8 characters long, includes numbers and upper/lower case, as well as a special character.
- School provided mobile phones and devices will always be used in accordance with the acceptable use of technology policy and other relevant policies.
- Staff with school provided mobile phones and devices will be informed prior to use via our Acceptable Use Policy (AUP) that activity may be monitored for safeguarding reasons and to ensure policy compliance.
- Work mobile phones may at times be needed to be used in the presence of pupils in order for the employee to do their job.

5 - Staff use of mobile and smart technology

- Members of staff will ensure that use of any mobile and smart technology, including personal phones and mobile devices, will take place in accordance with the law, as well as relevant school policy and procedures, such as confidentiality, child protection, data security, code of conduct and Acceptable Use Policies.
- Staff will be advised to:

- Keep personal mobile phones and personal devices in a safe and secure place (e.g. locker/draw) during lesson time.
- Keep personal mobile phones and devices switched off or set to 'silent' mode during lesson times.
- Ensure that Bluetooth or other forms of communication, such as 'airdrop', are hidden or disabled during lesson times.
- Not use personal devices during teaching periods unless permission has been given by the head teacher, such as in emergency circumstances.

- Personal mobile phones must not be used to contact pupils or parents at any time. During school outings, nominated staff will have access to a school mobile phone which can be used for emergency or contact purposes. If this is not possible the Headteacher will grant permission to the trip leader to use their personal phone to contact school or SLT if necessary.
- Personal mobile or smart devices are not allowed to join the main school WiFi to reduce the risk of cyber-security breaches.
- Staff will only use school provided equipment to:

  - take photos or videos of pupils in line with our image use policy.
  - work directly with pupils during lessons/educational activities.
  - communicate with parents/carers.

- Where remote learning activities take place, staff will use School provided equipment.
- If a member of staff breaches our policy, action will be taken in line with our Low-level concerns policy and staff disciplinary procedure. Any concerns should be immediately referred to the headteacher.
- If a member of staff is thought to have illegal content saved or stored on a mobile phone or personal device or have committed a criminal offence using a personal device or mobile phone, the police will be contacted and the LADO (Local Authority Designated Officer) will be informed in line with our staff disciplinary procedure.

5.1 Staff Smart watches

- Staff are allowed to use smartwatches, but they follow the same policy as mobile phones:
  - Staff are not to use their watch to send messages, photos, make phone calls or transfer any other kind of data whilst working with children. Any communications using their smartwatch must be during their own lunch/break time and away from children.
  - Staff are not permitted to take or store images of pupils on their smartwatch.
  - Personal information about staff, pupils or the school is not to be taken on a smartwatch.
  - Smartwatches are not allowed to join the school WiFi.
  - Notifications must be turned off whilst using your smartwatch at school.

6 - Pupil's use of mobile and smart technology

- Pupils will be educated regarding the safe and appropriate use of mobile and smart technology, including mobile phones and personal devices, and will be made aware of behaviour expectations and consequences for policy breaches.
- Mobile phones and/or personal devices will not be used on site by pupils at any time.
- Pupils in KS2 may bring in a mobile phone into school if needed for personal safety when walking independently to and from school. Parents and carers will need to complete an agreement that their child can bring a device into school.
    - Mobile phones or personal devices will not be allowed to be kept in the classroom; all devices must be handed into the office at the start of the day and collected at the end of the day. They must also be turned off.
    - Pupils will not be allowed to use their mobile phone or personal devices during the school day, this includes before and after-school whilst on school site.
    - Mobile phones and personal devices can only be used in the school day if agreed with the head teacher.

- If a pupil needs to contact their parents or carers whilst on site, they will be allowed to use a school phone in the office.
  Parents are only allowed to contact their child via the school office phone/email. Any exception must be agreed by the head teacher first.
- If a pupil requires access to a personal device in exceptional circumstances E.g disability-related reasonable adjustments, SEND and other individual circumstances, such as medical assistance and monitoring, this will be discussed with the head teacher, and a risk assessment put in place.
    - Any arrangements regarding access to personal devices in exceptional circumstances will be documented and recorded by the school.
    - Any exceptional circumstances agreements (including sanctions for misuse) will be provided in writing and agreed by the pupil and their parents/carers before use is permitted.
- Mobile phones and devices that have been confiscated will be held in a secure place and only released to parents/carers at the end of the day, unless subject to a police enquiry.

- Concerns regarding policy breaches by pupils will be shared with parents/carers as appropriate.

- Where there is a concern that a child is at risk of harm, we will contact respond in line with our child protection policy.

- If there is suspicion that material on a pupil's personal device or mobile phone may be illegal, or may provide evidence relating to a criminal offence, the device may need to be handed over to the police for further investigation. If a member of staff believes that there is inappropriate content on any device then the procedures relating to searching and confiscating, as laid out in

the child protection policy, will be followed. No staff member should confiscate or view or share anything held on a device without a member of the DSL team in attendance.

6.1 Pupil use of smartwatches

● Smartwatches will be discouraged from being brought into school. They will only be allowed in school under the following directive:

- Smartwatches with cellular data are not permitted.
- Smartwatches with cameras are not permitted.
- Mobile phones linked to smartwatches must be turned off and handed into the school office.
- Smartwatches follow the same policy as mobile phones and are not to be used during the school day, including before/after school whilst on site.

7 - Visitors' use of mobile and smart technology

- Parents/carers and visitors, including volunteers and contractors, are expected to ensure that:
  - Mobile phones are not to be used in the classroom or when around any children. Use of mobile phones should only be during break/lunch time and in private areas (i.e. staffroom or meeting rooms).
  - Personal devices will not be allowed to join the main school WiFi
  - Personal devices are not allowed to take or store images of pupils for any purpose.
  - Keep personal mobile phones and devices switched off or set to 'silent' mode during lesson times.
  - Ensure that Bluetooth or other forms of communication, such as 'airdrop', are hidden or disabled during lesson times.
- Appropriate signage and information are in place at the school entrance to inform visitors of our expectations for safe and appropriate use of personal devices and mobile phones.
- Visitors, including parents, volunteers and contractors are expected to use mobile and smart technology in accordance with our acceptable use of technology policy and other associated policies, including child protection.
- Members of staff are expected to challenge visitors if they have concerns about their use of mobile and smart technology and will inform the DSLs or head teacher of any breaches of our policy.

8 - Emerging online risks

King David Primary School recognises that emerging technologies, including generative artificial intelligence (AI), can create additional safeguarding risks. These include misleading or harmful content, inappropriate interactions with AI chatbots, and deepfakes, digitally altered or AI-generated images, audio or video, including sexual imagery depicting children.

Staff and pupils must not use technology to create or share abusive, exploitative or sexualised content. Any concern involving these technologies must be reported promptly to the Designated Safeguarding Lead (DSL) and managed in accordance with the school's Online Safety Policy and Child

Protection Policy. Suspected sexual imagery involving children must not be copied, forwarded or investigated by staff; advice must be sought immediately from the DSL.

The school will keep these risks under review and provide age-appropriate education and staff guidance to support safe use of technology.

9 - Policy monitoring and review

- Technology evolves and changes rapidly. King David will review this policy annually. The policy will be revised following any national or local policy updates, any local concerns and/or any changes to our technical infrastructure.
- We will regularly monitor internet use taking place via our provided devices and systems and evaluate online safety mechanisms to ensure that this policy is consistently applied. Any issues identified will be incorporated into our action planning. At King David all school devices are monitored using the SECURUS system with any serious breaches / concerns reported immediately to a DSL so appropriate action can be taken.

10 - Responding to policy breaches

- All members of the community are informed of the need to report policy breaches or concerns in line with existing school policies (Low level concerns and Whistleblowing) and procedures.
- After any investigations are completed, leadership staff will debrief, identify lessons learnt and implement any policy or curriculum changes, as required.
- We require staff, parents/carers, and pupils to work in partnership with us to resolve issues.
- All members of the community will respect confidentiality and the need to follow the official procedures for reporting concerns.
- Pupils, parents, and staff will be informed of our complaints procedure and staff will be made aware of the whistleblowing procedure.

Appendix 1

King David Primary School

Staff, Governors and Volunteer Acceptable Use Policy

New technologies have become integral to the lives of children and young people today, both within schools and in their lives outside school. The internet and other digital technologies are powerful tools, which open new opportunities for everyone. These technologies can stimulate discussion and promote creativity, promoting effective learning. They also bring opportunities for staff to be more creative and productive in their work.

This Acceptable Use Policy is intended to ensure:

- That staff and volunteers will be safe and responsible users of the internet and other digital technologies.
- That school ICT systems and users are protected from accidental or deliberate misuse.
- The school will try to ensure that staff and volunteers will have good access to ICT to enhance their work and improve opportunities for learners and will, in return, expect staff and volunteers to agree to be responsible users.

Acceptable Use Policy Agreement:

- I understand that I must use school ICT systems in a responsible way, to minimise the risk to my safety or to the safety and security of the ICT systems and other users. I will, where possible, educate the young people in my care in the safe use of ICT and embed e-safety in my work with young people.

For my professional and personal safety:

- I understand that the school will monitor my use of its ICT systems including email and other digital communications technologies.
- I understand that this agreement also apply to use of school ICT systems out of school (eg laptops, email, VLP etc).
- I understand that the school ICT systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school.
- I will keep my usernames and passwords private and will not try to use anyone else's username and password.
- I will immediately report any illegal, inappropriate or harmful material or incident, to the appropriate person in school.

I will be professional in my communications and actions when using school ICT systems:

- I will not access, copy, delete or otherwise alter any other user's files, without their permission.
- I will communicate with others in a professional manner.

- I will ensure that when I take or publish images of pupils or parents/colleagues, I will do so with their permission and in accordance with the school's policy. I will not use my personal equipment to record these images. Where these images are published (eg on the school website / VLP) it will not be possible to identify pupils by name, or other personal information.
- I will only use chat and social networking sites in school in accordance with school policy.
- I will only communicate with pupils and parents / carers using official school systems and in a professional manner. I will not share any personal information with a pupil (including personal phone numbers or email address). Nor will I request or respond to any personal information from a young person unless it is appropriate as part of my professional role.
- I will not engage in any on-line activity that may compromise my professional responsibilities.

The school and the local authority have the responsibility to provide safe and secure access to technologies:

- When I use my personal handheld/external devices in school (laptops/mobile phones/USB devices etc), I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules set by the school about such use. I will ensure that when connecting these devices to school ICT systems, they are protected by up-to-date anti-virus software and are free from viruses.
- I will not use personal email addresses on the school ICT systems.
- I will not open any attachments to emails, unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful programmes.
- I will ensure that my data is regularly backed up, in accordance with relevant school policies.
- I will not try to upload, download or access any material which is illegal or inappropriate or may cause harm or distress to others (e.g. child sexual abuse images, criminally racist material, adult pornography etc). I will not try to use any programmes or software that might allow me to bypass the filtering / security systems intended to prevent access to such materials.
- Unless I have permission, I will not try to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on school systems, nor will I try to alter computer settings, unless this is allowed in school policies.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School Data Protection Policy. Where personal data is electronically transferred outside the secure school network, it must be encrypted.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the internet in my professional capacity or for school sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work.
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

I understand that I am responsible for my actions in and out of school:

- I understand that this Acceptable Use Policy applies not only to my work and use of school ICT equipment in school but also applies to my use of school ICT systems and equipment out of school and my use of personal equipment in school or in situations related to my employment by the school.
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action and in the event of illegal activities, the involvement of the police.

I have read and understand the above and agree to use the school ICT systems both in and out of school and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Name _____

Signed _____ Date _____