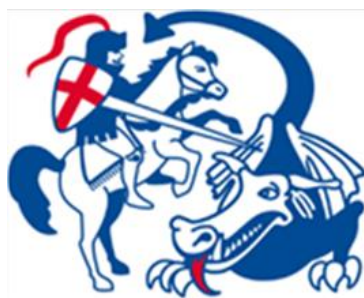


Mobile Technology and Social Media Policy

Reviewed on: September 2020

Next review: September 2021

**St. George's CE Primary School
Wrotham, Kent**



Designated Safeguarding Leads:

Designated Safeguarding Lead: **Mrs Elizabeth Rye, Headteacher**

Deputy Designated Safeguarding Lead: **Mr Matthew Jones, Deputy Headteacher**

Named Safeguarding Governor with lead responsibility:

Mrs Sandy Chapman, Chair of Worship, Inclusion & Safeguarding

Date written: (September 2020)

Date agreed and ratified by Governing Body: (November 2020)

Date of next review: (September 2021)

1. Policy aims

- 1.1 The mobile technology and social media policy has been written **by St. George's CE Primary School** involving staff, learners and parents/carers, building on The Education People policy template, with specialist advice and input as required.
- 1.2 It takes into account the DfE statutory guidance '[Keeping Children Safe in Education](#)' 2020, [Early Years and Foundation Stage](#) 2017 '[Working Together to Safeguard Children](#)' 2018 and the local [Kent Safeguarding Children Multi-agency Partnership](#) (KSCMP) procedures.
- 1.3 **St. George's CE Primary School** is currently operating in response to coronavirus (Covid-19); our safeguarding principles in accordance with 'Keeping Children Safe in Education' (KCSIE) 2020 and related guidance, however, remain the same.
 - Where children are asked to learn online at home in response to a full or partial closure, **St. George's CE Primary School** will follow expectations as set out within the Child Protection Policy and Remote Learning AUP and in line with DfE Guidance, '[Safeguarding and remote education during coronavirus \(COVID-19\)](#)' 2020.
- 1.4 The purpose of **St. George's CE Primary School** mobile technology and social media policy is to safeguard and promote the welfare of all members of **St. George's CE Primary School** community when using mobile devices or social media on site and at home.
- 1.5 **St. George's CE Primary School** recognises that online safety is an essential part of safeguarding and acknowledges its duty to ensure that all learners and staff are protected from potential harm when using mobile technology or social media.
- 1.6 **St. George's CE Primary School** identifies that the mobile devices, such as computers, tablets, mobile phones, smart watches and games consoles, and social media, are an important part of everyday life, which present positive and exciting opportunities, as well as challenges and risks.
- 1.7 **St. George's CE Primary School** will empower our learners to acquire the knowledge needed to use the mobile technology and social media in a safe, considered and respectful way, and develop their resilience so they can manage and respond to online risks.

2. Policy scope

- 2.2 This policy applies to learners, 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).
- 2.3 This policy applies to all access to and use of mobile technology and social media, both on and off-site.

3. Links with other policies

- 3.1 This policy links with several other policies, practices and action plans, including but not limited to:
- Anti-bullying policy
 - Acceptable Use Policies (AUP) and/or the Code of conduct
 - Behaviour policy
 - Cameras and image use policy
 - Child protection policy
 - Confidentiality policy
 - Curriculum policies, such as: Computing, Personal Social and Health Education (PSHE), Citizenship and Relationships and Sex Education (RSE)
 - Data security
 - Searching, screening and confiscation policy

4. Monitoring and review

- 4.1 Technology evolves and changes rapidly. **St. George's CE Primary School** will review this policy at least annually. The policy will be revised following any national or local policy updates, any local child protection concerns and/or any changes to our technical infrastructure.
- 4.2 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.
- 4.3 To ensure they have oversight of online safety, the *headteacher* will be informed of online safety concerns, as appropriate.
- 4.4 The named governor for safeguarding will report on online safety practice and incidents, including outcomes, on a regular basis to the wider governing body..
- 4.5 Any issues identified via monitoring policy compliance will be incorporated into our action planning.

5. Responding to policy breaches

- 5.1 All members of the community will be made aware of how the *school* will monitor policy compliance through staff training, classroom management, Child Protection policy, AUP
- 5.2 All members of the community are informed of the need to report policy breaches or concerns in line with existing *school* policies and procedures such as Child Protection policy, AUP
- 5.3 All members of the community will respect confidentiality and the need to follow the official procedures for reporting concerns.
- 5.4 Learners, parents and staff will be informed of our complaints procedure and staff will be made aware of the whistleblowing procedure.
- 5.5 We require staff, parents/carers and learners to work in partnership with us to resolve issues.
- 5.6 If appropriate, after any investigations are completed, leadership staff will debrief, identify lessons learnt and implement any policy or curriculum changes, as required.

- 5.7 If we are unsure how to proceed with an incident or concern, the DSL (or deputy) or *headteacher* will seek advice from the [Education People's Education Safeguarding Service](#) or other agency in accordance with our child protection policy.
- 5.8 Where there is a concern that illegal activity has taken place, we will contact the police using 101, or 999 if there is immediate danger or risk of harm.

1. Mobile Technology: Use of Personal Devices and Mobile Phones in St. George's CE Primary School

6.1 Expectations

- 6.1.1 **St. George's CE Primary School** recognises that personal communication through mobile technologies is part of everyday life for many learners, staff and parents/carers. Mobile technology needs to be used safely and appropriately within the setting.
- 6.1.2 All use of mobile technology, including 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 imagery), will take place in accordance with our policies, such as anti-bullying, behaviour and child protection and with the law.
- 6.1.3 Electronic devices of any kind that are brought onto site are the responsibility of the user. All members of **St. George's CE Primary School** community 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 passwords/pin numbers to ensure that unauthorised calls or actions cannot be made on their phones or devices; passwords and pin numbers should be kept confidential and mobile phones and personal devices should not be shared
- 6.1.4 Mobile phones and personal devices are not permitted to be used in specific areas on site, such as: classrooms, changing rooms and toilets
- 6.1.5 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 and behaviour policies.
- 6.1.6 All members of **St. George's CE Primary School** community are advised to ensure that their mobile phones and personal devices do not contain any content which may be offensive, derogatory or would otherwise contravene our AUP, Code of conduct, behaviour or child protection policies.

6.2 Staff use of personal devices and mobile phones

- 6.2.1 Members of staff will ensure that use of any personal phones and mobile devices will take place in accordance with the law, as well as relevant policy and procedures, such as confidentiality, child protection, data security, acceptable use of technology and staff code of conduct
- 6.2.2 Staff will be advised to
- keep mobile phones and personal devices in a safe and secure place (in a classroom cupboard) during lesson time.

- keep mobile phones and personal devices switched off or switched 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 *headteacher* such as in emergency circumstances.
- ensure that any content bought onto site via mobile phones and personal devices are compatible with their professional role and expectations.

6.2.3 Members of staff are only permitted to use their own personal phones or devices for contacting learners or parents and carers to use Class Dojo

- Any pre-existing relationships which could undermine this, will be discussed with the DSL (or deputy) and *headteacher*.

6.2.4 Staff will only use *school* provided equipment (not personal devices):

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

6.2.5 Where remote learning activities because of Covid-19, staff will use *school* provided equipment. If this is not available, staff will only use personal devices with prior approval from the *headteacher*, following a formal risk assessment. Staff will follow clear guidance outlined in the *acceptable use policy and remote learning AUP*.

6.2.6 If a member of staff breaches our policy, action will be taken in line with our staff behaviour and allegations policy.

6.2.7 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 allegations policy.

6.3 Learners use of personal devices and mobile phones

6.3.1 Learners will be educated regarding the safe and appropriate use of personal devices and mobile phones and will be made aware of boundaries and consequences.

6.3.2 **St. George's CE Primary School** expects learners' personal devices and mobile phones to be handed into the school office until the end of the day.

6.3.3 If a learner needs to contact his/her parents or carers whilst on site, they will be allowed to use a *school* phone with supervision of a staff member

- Parents are advised to contact their child via the school office

6.3.4 Where learners' mobile phones or personal devices are used when learning at home, such as in response to local or full lockdowns, this will be in accordance with our *Acceptable Use Policy and/or Remote Learning AUP*.

6.3.5 Any concerns regarding learners use of mobile technology or policy breaches will be dealt with in accordance with our existing policies, including anti-bullying, child protection and behaviour.

- Staff may confiscate a learner's mobile phone or device if they believe it is being used to contravene our child protection, behaviour or anti-bullying policy.
- Searches of mobile phone or personal devices will be carried out in accordance with [‘Searching, Screening and Confiscation’](#) guidance.
- Mobile phones and devices that have been confiscated will be held in a secure place and released to parents/ carers. e.g. in the school office, at the end of the day
- Appropriate sanctions and/or pastoral/welfare support will be implemented in line with our behaviour policy.
- Concerns regarding policy breaches by learners will be shared with parents/carers as appropriate.
- If there is suspicion that material on a learner's personal device or mobile phone may be illegal, or may provide evidence relating to a criminal offence, the device will be handed over to the police for further investigation.

6.4 Visitors' use of personal devices and mobile phones

- 6.4.1 Parents/carers and visitors, including volunteers and contractors, should ensure that mobile phones are only permitted to be used if attending a class worship, production and specific guidance has been given by the school
- 6.4.2 Visitors, including volunteers and contractors, who are on site for regular or extended periods of time are expected to use their mobile phones and personal devices in accordance with our acceptable use of technology policy and other associated policies, including but not limited to anti-bullying, behaviour, child protection and image use.
- 6.4.3 Members of staff are expected to challenge visitors if they have concerns and inform the DSL (or deputy) or [headteacher](#) of any breaches of our policy.
- 6.4.4 Where staff or learners are using [school/setting](#) provided mobile phones and/or devices, they will be informed prior to use that activity may be monitored for safeguarding reasons and to ensure policy compliance.
- 6.4.5 [School/setting](#) mobile phones and devices will always be used in accordance with the acceptable use of technology policy and other relevant policies. **List others as appropriate.**

7. Use of Social Media in St. George's CE Primary School

7.1 Expectations

- 7.1.1 The expectations' regarding safe and responsible use of social media applies to all members of **St. George's CE Primary School** community.
- 7.1.2 The term social media may include (but is not limited to) blogs, wikis, social networking sites, forums, bulletin boards, online gaming, apps, video/photo sharing sites, chatrooms and instant messenger apps or services.
- 7.1.3 All members of **St. George's CE Primary School** community are expected to engage in social media in a positive and responsible manner.
- 7.1.4 All members of **St. George's CE Primary School** community are advised not to post or share content that may be considered threatening, hurtful or defamatory to others on any social media service.
- 7.1.5 We will control learner and staff access to social media whilst using *school* provided devices and systems on site using appropriate filtering and monitoring systems (*see AUP*)
- 7.1.6 The use of social media during *school* hours for personal use *is only* permitted for staff during breaks in places where there are no children present .
- 7.1.7 Inappropriate or excessive use of social media during *school* hours or whilst using *school* devices may result in removal of internet access and/or disciplinary action.
- 7.1.8 The use of social media or apps as a formal remote learning platform following Covid-19 restrictions will be robustly risk assessed by the DSL and/or *headteacher* prior to use by staff or learners. The use of such platforms will only take place in accordance with our *remote learning acceptable use policy*.
- 7.1.9 Concerns regarding the online conduct of any member of **St. George's CE Primary School** community on social media, will be reported to the DSL and/or *headteacher* and will be managed in accordance with existing policies, including anti-bullying, allegations against staff, behaviour and child protection.

7.2 Staff personal use of social media

- 7.2.1 The safe and responsible use of social media sites will be discussed with all members of staff as part of staff induction and will be revisited and communicated via regular staff training opportunities.
- 7.2.2 Safe and professional online behaviour is outlined for all members of staff, including volunteers, as part of our *code of conduct and acceptable use of technology policy*.
- 7.2.3 Any complaint about staff misuse or policy breaches will be referred to the headteacher, in accordance with our allegations against staff policy.
- 7.2.4 Any allegations regarding a member of staff's online conduct will be discussed with the LADO (Local Authority Designated Officer).
- 7.2.5 If appropriate, disciplinary, civil and/or legal action will be taken in accordance with our staff *code of conduct*.

Reputation

- 7.2.6 All members of staff are advised that their online conduct on social media can have an impact on their role and reputation within the *school*.
- 7.2.7 Civil, legal or disciplinary action may be taken if staff are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.
- 7.2.8 All members of staff are advised to safeguard themselves and their privacy when using social media services. Advice will be provided via staff training; additional guidance and resources will be shared with staff on a regular basis. This will include, but is not limited to:
- Setting appropriate privacy levels on their personal accounts/sites.
 - Being aware of the implications of using location sharing services.
 - Opting out of public listings on social networking sites.
 - Logging out of accounts after use.
 - Using strong passwords.
 - Ensuring staff do not represent their personal views as being that of the setting.
- 7.2.9 Members of staff are encouraged not to identify themselves as employees of **St. George's CE Primary School** on their personal social networking accounts; this is to prevent information being linked with the setting and to safeguard the privacy of staff members.
- 7.2.10 All members of staff are encouraged to carefully consider the information, including text and images, they share and post online. Staff are expected to ensure that their social media use is compatible with their professional role and is in accordance our policies, and the wider professional and legal framework.
- 7.2.11 Information and content that staff members have access to as part of their employment, including photos and personal information about learners and their family members or colleagues, will not be shared or discussed on social media sites.
- 7.2.12 Members of staff will notify the leadership team immediately if they consider that any content shared on social media sites conflicts with their role.

Communicating with learners and parents/carers

- 7.2.13 Staff will not use any personal social media accounts to contact learners or parents/carers, nor should any contact be accepted.
- 7.2.14 All members of staff are advised not to communicate with or add any current or past learners or their family members, as 'friends' on any personal social media sites, applications or profiles.
- 7.2.15 Any pre-existing relationships or exceptions which compromise this requirement will be discussed with the DSL and/or the *headteacher*
- 7.2.16 Decisions made and advice provided in these situations will be formally recorded to safeguard learners, members of staff and the setting.
- 7.2.17 If ongoing contact with learners is required once they have left the setting, members of staff will be expected to use existing alumni networks, or use official setting provided communication tools.

7.2.18 Any communication from learners and parents received on personal social media accounts will be reported to the DSL (or deputy) *and/or* the *headteacher*

7.3 Learners use of social media

7.3.1 Safe and appropriate use of social media will be taught to learners as part of an embedded and progressive educational approach using age appropriate sites and resources. Further information is contained within our curriculum policies: *e.g. RSE and Computing*.

7.3.2 We are aware that many popular social media sites are not permitted for use by children under the age of 13, or in some cases higher. As such, we will not create accounts for learners under the required age as outlined in the services terms and conditions.

7.3.3 Learners will be advised:

- to consider the benefits and risks of sharing personal details or information on social media sites which could identify them and/or their location.
- to only approve and invite known friends on social media sites and to deny access to others by making profiles private.
- not to meet any online friends without a parent/carer or other appropriate adults' permission, and to only do so when a trusted adult is present.
- to use safe passwords.
- to use social media sites which are appropriate for their age and abilities.
- how to block and report unwanted communications.
- how to report concerns on social media, both within the setting and externally.

7.3.4 Any concerns regarding learners use of social media will be dealt with in accordance with existing policies, including anti-bullying, child protection and behaviour.

7.3.5 The DSL (or deputy) will respond to online safety concerns involving safeguarding or child protection risks in line with our child protection policy.

7.3.6 Sanctions and/or pastoral/welfare support will be implemented and offered to learners as appropriate, in line with our behaviour policy. Civil or legal action will be taken if necessary.

7.3.7 Concerns regarding learners use of social media will be shared with parents/carers as appropriate, particularly when concerning underage use of social media services and games.

7.4 Official use of social media

7.4.1 **St. George's CE Primary School** official social media channels are a *Twitter link*

7.4.2 The official use of social media sites by **St. George's CE Primary School** only takes place with clear educational or community engagement objectives and with specific intended outcomes.

7.4.3 The official use of social media as a communication tool has been formally risk assessed and approved by the *headteacher*.

7.4.4 Leadership staff have access to account information and login details for our social media channels, in case of emergency, such as staff absence.

7.4.5 Official social media channels have been set up as distinct and dedicated accounts for official educational or engagement purposes only.

- 7.4.6 Staff use setting provided email addresses to register for and manage official social media channels.
- 7.4.7 Official social media sites are suitably protected and, where possible, run *and/or* linked *to/from* our website.
- 7.4.8 Public communications on behalf of the setting will, where appropriate and possible, be read and agreed by at least one other colleague.
- 7.4.9 Official social media use will be conducted in line with existing policies, including but not limited to anti-bullying, image/camera use, data protection, confidentiality and child protection.
- 7.4.10 All communication on official social media platforms by staff on behalf of the setting will be clear, transparent and open to scrutiny.
- 7.4.11 Parents/carers and learners will be informed of any official social media use, along with expectations for safe use and action taken to safeguard the community.
- 7.4.12 Only social media tools which have been risk assessed and approved as suitable for educational purposes will be used.
- 7.4.13 Any official social media activity involving learners will be moderated if possible.
- 7.4.14 Parents and carers will be informed of any official social media use with learners; written parental consent will be obtained, as required.
- 7.4.15 We will ensure that any official social media use does not exclude members of the community who are unable or unwilling to use social media channels.
- 7.4.16 Members of staff who follow and/or like our official social media channels will be advised to use dedicated professional accounts where possible, to avoid blurring professional boundaries.
- 7.4.17 If members of staff are participating in online social media activity as part of their capacity as an employee of the setting, they will:
- Be aware they are an ambassador for the setting.
 - Be professional, responsible, credible, fair and honest, and consider how the information being published could be perceived or shared.
 - Always act within the legal frameworks they would adhere to within the workplace, including libel, defamation, confidentiality, copyright, data protection and equalities laws.
 - Ensure appropriate consent has been given before sharing images on the official social media channel.
 - Not disclose information, make commitments or engage in activities on behalf of the setting, unless they are authorised to do so.
 - Not engage with any private/direct messaging with current or past learners or parents/carers.
 - Inform their line manager, the DSL (or deputy) and/or the *headteacher* of any concerns, such as criticism, inappropriate content or contact from learners.