

LITTLEBOURNE CE PRIMARY SCHOOL



Online Safety Policy

Key Contact Personnel in School

Headteacher: Samantha Killick

Chair of Governors: Anna Webber

Date Written: March 2023

Date of Next Review: March 2024

Designated Safeguard Lead: Samantha Killick,
Headteacher;

Deputy DSLs: Charlotte McLean, SENDCo; Kay Pott,
SBM

Name Governor with Lead Responsibility: Claire Ledger

1. Policy aims and scope

This policy has been written by *Littlebourne Church of England Primary School* involving staff, children/pupils/students and parents/carers, building on The Education People's mobile and smart technology policy template with specialist advice and input as required, taking into account the DfE statutory guidance '[Keeping Children Safe in Education](#)' 2022, [Early Years and Foundation Stage](#) 2021 '[Working Together to Safeguard Children](#)' 2018, '[Behaviour in Schools Advice for headteachers and school staff](#)' 2022, and the local [Kent Safeguarding Children Multi-agency Partnership](#) (KSCMP) procedures.

- The purpose of this policy is to safeguard and promote the welfare of all members of the Littlebourne community when using mobile devices and smart technology.
 - Littlebourne recognises that online safety is an essential part of safeguarding and acknowledges its duty to ensure that all children 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), *Samantha Killick, Headteacher*, is recognised as having overall responsibility for online safety.
- This policy applies to all access to and use of all 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 and/or images.
- This policy applies to children, 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:
 - Anti-bullying policy
 - Acceptable Use Policies (AUP)
 - Behaviour policy
 - Child protection policy
 - Code of conduct
 - Data security
 - Social media

3. Safe use of mobile and smart technology expectations

- Littlebourne recognises that use of mobile and smart technologies is part of everyday life for many children, staff and parents/carers.
- Electronic devices of any kind that are brought onto site are the responsibility of the user. All members of the Littlebourne 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 access, calls or actions cannot be made on their phones or devices.
- Mobile phones and personal devices are not permitted to be used in specific areas on site, such as changing rooms, toilets and swimming pools or other areas accessed by the children.
- The sending of abusive or inappropriate messages or content, including via personal smart devices and mobile phones 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 the Littlebourne community 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

- Staff providing formal remote/online learning will do so using school provided equipment in accordance with our Acceptable Use Policy (AUP)
- School mobile phones and devices will be suitably protected via a passcode/password/PIN and must only be accessed or used by members of staff and/or children.
- School mobile phones and devices will always be used in accordance with our staff code of conduct.
- Where staff and/or children are using school provided mobile phones and/or devices, they 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.

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 staff code of conduct and Acceptable Use Policies.
- Staff will be advised to:
 - Keep mobile phones and personal devices in a safe and secure place (designated lockers, the staffroom, the main school office or the Headteacher's office) 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 written permission has been given by the headteacher, such as in emergency circumstances.
- Ensure that any content bought onto site via personal mobile phones and devices is compatible with their professional role and our behaviour expectations.
- Members of staff are not permitted to use their own personal phones or devices for contacting children or parents and carers.
 - Any pre-existing relationships or circumstance, which could compromise staff's ability to comply with this, will be discussed with the DSL or headteacher.
- Staff will only use school provided equipment (not personal devices):
 - to take photos or videos of children in line with our image use policy.
 - to work directly with children during lessons/educational activities.
 - to communicate with parents/carers.
- Where remote learning activities take place, 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.
- If a member of staff breaches our policy, action will be taken in line with our staff code of conduct and allegations policy.
- 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. Children's use of mobile and smart technology

Children 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.

- Safe and appropriate use of mobile and smart technology will be taught to children as part of an embedded and progressive safeguarding education approach using age-appropriate sites and resources. Further information is contained within our Child Protection policy
- Mobile phones and/or personal devices will not be used on site by children
- If a child needs to contact their parents or carers whilst on site, they will be allowed to visit the school office where Mrs Pott will use a school phone.
 - Parents are advised to contact their child via the school office
- If a child requires access to a personal device in exceptional circumstances, for example medical assistance and monitoring, this will be discussed with the headteacher prior to use being permitted.

- Any arrangements regarding access to personal devices in exceptional circumstances will be documented and recorded by the school.
- Any specific agreements and expectations (including sanctions for misuse) will be provided in writing and agreed by the learner and their parents/carers before use is permitted.
- Where children mobile phones or personal devices are used when learning at home, this will be in accordance with our Acceptable Use Policy. This includes the use of any home - school communication applications such as Weduc, or Parent Mail. Any inappropriate use or misuse of these applications will result in immediate action being taken by the school and potential restriction of use.
- Mobile phones and personal devices must not be taken into examinations. Children found in possession of a mobile phone or personal device which facilitates communication or internet access during an exam will be reported to the appropriate examining body. This may result in the withdrawal from either that examination or all examinations.

6.1 Screening, searching and confiscation of electronic devices

- Electronic devices, including mobile phones, can contain files or data which relate to an offence, or which may cause harm to another person. This includes, but is not limited to, indecent images of children, pornography, abusive messages, images or videos, or evidence relating to suspected criminal behaviour.
- Where there are any concerns regarding children's use of mobile technology or policy breaches, they will be dealt with in accordance with our existing policies, including anti-bullying, child protection, and behaviour.
- Staff may confiscate a child's mobile phone or device if they believe it is being used to contravene our child protection or behaviour or anti-bullying policy.
- Mobile phones and devices that have been confiscated will be held in the school office and released to parents/carers at the end of the day.
- Where a concern involves a potentially indecent image or video of a child, staff will respond in line with our child protection policy and will confiscate devices, avoid looking at any content, and refer the incident to the Designated Safeguarding Lead (or deputy) urgently as they will be most appropriate person to respond.
- If there is suspicion that data or files on a child'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
- If deemed to be necessary and appropriate, searches of mobile phones or personal devices may be carried out in accordance with the DfE '[Searching, Screening and Confiscation](#)' guidance.
- Staff will respond in line with our child protection policy and follow the most appropriate safeguarding response if they find images, data or files on a pupil's electronic device that they reasonably suspect are likely to put a person at risk.

- The Designated Safeguarding Lead (or deputy) will always be informed of any searching incidents where authorised members of staff have reasonable grounds to suspect a pupil was in possession of prohibited items, as identified in our behaviour policy.
- The Designated Safeguarding Lead (or deputy) will be involved without delay if staff believe a search of a pupil's device has revealed a safeguarding risk.
- In exceptional circumstances and in accordance with our behaviour policy and the DfE [‘Searching, Screening and Confiscation’](#) guidance, the headteacher or authorised members of staff may examine or erase data or files if there is a good reason to do so.
- If the headteacher or a member of staff finds any data or files that they suspect might constitute a specified offence, they will be delivered to the police as soon as is reasonably practicable.

7. Visitors’ use of mobile and smart technology

- Parents/carers and visitors, including volunteers and contractors, are expected to ensure that:
 - *mobile phones are only used within specific areas*
- Appropriate signage and information are in place (*posters along with face to face information* to inform visitors of our expectations for safe and appropriate use of personal devices and mobile phones).
- Visitors, including volunteers and contractors, who are on site for regular or extended periods of time are expected to use mobile and smart technology in accordance with our acceptable use of technology policy and other associated policies, including child protection.
- If visitors require access to mobile and smart technology, for example when working with children as part of multi-agency activity, this will be discussed with the headteacher prior to use being permitted.
 - Any arrangements regarding agreed visitor access to mobile/smart technology will be documented and recorded by the school. This may include undertaking appropriate risk assessments if necessary.
- Members of staff are expected to challenge visitors if they have concerns about their use of mobile and smart technology and will inform the DSL or headteacher of any breaches of our policy.

8. Policy monitoring and review

- Technology evolves and changes rapidly. Littlebourne will review this policy at least 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.
- All members of the community will be made aware of how the school will monitor policy compliance: This will be achieved through staff training and classroom management.

9. 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 and procedures. This includes Child Protection Policy and Code of Conduct.
- Where children breach this policy:
 - appropriate sanctions and/or pastoral/welfare support will be implemented in line with our behaviour policy.
 - concerns will be shared with parents/carers as appropriate.
 - we will respond in line with our child protection policy, if there is a concern that a child is at risk of harm.
- 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 children 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.
- Children's parents and staff will be informed of our complaints procedure and staff will be made aware of the whistleblowing procedure.
- If we are unsure how to proceed with an incident or concern, the DSL (or a deputy) or headteacher will seek advice from the [Education People's Education Safeguarding Service](#) or other agency in accordance with our child protection policy.

Social Media Policy

1. Policy aims and scope

- This policy has been written by Littlebourne CEP School involving staff, children/pupils/students and parents/carers, building on The Education People's social media policy template with specialist advice and input as required, taking into account the DfE statutory guidance '[Keeping Children Safe in Education](#)' 2021, '[Early Years and Foundation Stage](#) 2021', '[Working Together to Safeguard Children](#)' 2018, '[Behaviour in Schools Advice for headteachers and school staff](#)' 2022, and the local '[Kent Safeguarding Children Multi-agency Partnership](#)' (KSCMP) procedures.
- The purpose of this policy is to safeguard and promote the welfare of all members of Littlebourne community when using social media.
 - Littlebourne recognises that online safety is an essential part of safeguarding and acknowledges its duty to ensure that all children and staff are protected from potential harm when using social media.
 - As outlined in our child protection policy, the Designated Safeguarding Lead (DSL), Samantha Killick, Headteacher, is recognised as having overall responsibility for online safety.
- The policy applies to all use of social media; the term social media includes, 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 other online communication services.
- This policy applies to children, 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:
 - Anti-bullying policy
 - Acceptable Use Policies (AUP)
 - Behaviour policy
 - Cameras and image use policy
 - Child protection policy
 - Code of conduct policy
 - Data security

3. General social media expectations

- Littlebourne believes everyone should be treated with kindness, respect and dignity. Even though online spaces may differ in many ways, the same standards of behaviour are expected online as offline and all members of the Littlebourne community are expected to engage in social media in a positive and responsible manner.
- All members of the Littlebourne community are advised not to post or share content that may be considered threatening, hurtful or defamatory to others on any social media service.
- We will control learner and staff access to social media whilst using school provided devices and systems on site. We use appropriate filtering and monitoring systems provided and monitored by SNS. If any attempts are made to access inappropriate or harmful material online, the safeguarding team are notified. All of the safeguarding team receive this notification.
- 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.
- The use of social media or apps, for example as a formal remote learning platform will be robustly risk assessed by the DSL and/or headteacher prior to use. Any use will take place in accordance with our Acceptable Use Policy.
- Concerns regarding the online conduct of any member of Littlebourne community on social media will be taken seriously. Concerns will be managed in accordance with the appropriate policies, including anti-bullying, allegations against staff, behaviour, home school-agreements, staff code of conduct, Acceptable Use Policies, and child protection.

4. Staff use of social media

- The use of social media during school hours for personal use is not permitted for staff unless this takes place during a lunch break.
- Safe and professional online behaviour is outlined for all members of staff, including volunteers, as part of our code of conduct and the acceptable use of technology policy.
- The safe and responsible use of social media sites will be discussed with all members of staff as part of staff induction. Advice will be provided and updated via staff training and additional guidance and resources will be shared with staff as required on a regular basis.
- Any complaint about staff misuse of social media or policy breaches will be taken seriously in line with our child protection and allegations against staff policy.

4.1 Reputation

- 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. 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.
- All members of staff are advised to safeguard themselves and their privacy when using social media. This may 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 school.
- Members of staff are encouraged not to identify themselves as employees of Littlebourne on their personal social networking accounts; this is to prevent information being linked with the setting and to safeguard the privacy of staff members.
 - All 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 reputation and legal framework. All members of staff are encouraged to carefully consider the information, including text and images, they share and post on social media.
 - Information and content that staff members have access to as part of their employment, including photos and personal information about children and their family members or colleagues, will not be shared or discussed on social media sites.
 - Members of staff will notify the leadership team immediately if they consider that any content shared on social media sites conflicts with their role.

4.2 Communicating with children and their families

- Staff will not use any personal social media accounts to contact children or their family members.
- All members of staff are advised not to communicate with or add any current or past children or their family members, as 'friends' on any personal social media accounts.
- Any communication from children and parents/carers received on personal social media accounts will be reported to the DSL (or deputy) and/or the headteacher.
- Any pre-existing relationships or situations, which mean staff cannot comply with this requirement, will be discussed with the DSL and the headteacher. Decisions made and advice provided in these situations will be formally recorded to safeguard children, members of staff and the setting.
- If ongoing contact with children 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.

5. Children's use of social media

- The use of social media during school hours for personal use is not permitted for children.
- Many online behaviour incidents amongst children and young people occur on social media outside the school day and off the school premises. Parents/carers are responsible for this behaviour; however, some online incidents may affect our culture and/or pose a risk to children and young people's health and well-being. Where online behaviour online poses a

threat or causes harm to another child, could have repercussions for the orderly running of the school when the child is identifiable as a member of the school, or if the behaviour could adversely affect the reputation of the school, action will be taken in line with our behaviour and child protection policies.

- Littlebourne will empower our children to acquire the knowledge needed to use social media in a safe, considered and respectful way, and develop their resilience so they can manage and respond to online risks. Safe and appropriate use of social media will be taught to children as part of an embedded and progressive safeguarding education approach using age-appropriate sites and resources. Further information is contained within our child protection and relevant specific curriculum policies.
- 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 children under the required age as outlined in the services terms and conditions.
- Children 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, for example 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.
- Any concerns regarding children's use of social media will be dealt with in accordance with appropriate existing policies, including anti-bullying, child protection and behaviour.
- The DSL (or deputy) will respond to social media concerns involving safeguarding or child protection risks in line with our child protection policy.
- Sanctions and/or pastoral/welfare support will be implemented and offered to children as appropriate, in line with our child protection and behaviour policy. Civil or legal action may be taken if necessary.
- Concerns regarding children's use of social media will be shared with parents/carers as appropriate, particularly when concerning underage use of social media services and games.

6. Policy monitoring and review

- Technology evolves and changes rapidly. Littlebourne will review this policy at least 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.

- All members of the community will be made aware of how the school will monitor policy compliance: This is achieved via staff training and classroom management.

7. 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 and procedures. This includes: Child Protection Policy and Code of Conduct Policy.
- 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 children 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.
- Children, parents and staff will be informed of our complaints procedure and staff will be made aware of the whistleblowing procedure.
- If we are unsure how to proceed with an incident or concern, the DSL (or a deputy) or headteacher will seek advice from the [Education People's Education Safeguarding Service](#) or other agency in accordance with our child protection policy.